Records Policy Manual

Volume 1 - General Records

Part A - Overview

Chapter 1 - Introduction

1. The Records Policy Manual (RPM) provides immigration personnel with the information necessary for compliance with government record keeping and information management.
2. The objectives of the RPM are to:
   a. Publish complete and accurate records guidance reflecting the policies and procedures for U.S. Citizenship and Immigration Services (USCIS) immigration records;
   b. Ensure that guidance is current; and
   c. Publish guidance efficiently and in a user-friendly manner.
3. The RPM is not static. It is a living document. As the needs of the organization change, so does the RPM. In addition, Identity and Information Management Division (IIMD) continues to add guidance in areas where there has not been previous formal guidance.
4. The RPM applies to Department of Homeland Security (DHS) employees, contractors, and anyone who creates or uses immigration records.
5. The information in this Part implements the policy found in DHS Management Directive 550-1 and the DHS Records Management Handbook.

Chapter 2 - Using the RPM

1. The RPM is accessible through IIMD USCIS Connect homepage and best viewed online.
2. The RPM is a living document and should not be printed, in part or in whole, as it is subject to frequent changes.
3. In most cases, the RPM does not define terms and acronyms in the text of the Part. Acronyms can be found at the end of the manual, and definitions can be found on the RPM Dictionary.
4. The RPM has hyperlinks to other documents, sites on the intranet and internet, and to material within the RPM.
5. Operational guidance can be found in the Consolidated Handbook of Adjudication Procedures (CHAP) or local SOPs.

Chapter 3 - Updating the RPM

1. IIMD updates the RPM regularly. The last revision date is provided in the footer of the RPM itself with policy updates notated in the Table of Revisions.

2. The RPM revision process is outlined in the RPM Working Group Charter. The process affords all operational components the opportunity to evaluate and assess operational impact prior to implementation of revised or new policy ensuring compliance once implemented.
3. RPM changes are made for a number of reasons, including:
   a. Adoption of better practices;
   b. Field personnel requests;
   c. Changes in the organization or operating needs; and/or
   d. Audit findings.
4. Policy updates are sent to the field via a broadcast message announcing the update. To receive the messages, you must be registered through GovDelivery.com.
5. All requests for changes, updates, or additions to the RPM, must be submitted online through the RPM Updates/Suggestions Form.

Part B - Basic Records Definitions and Concepts

Chapter 1 - Introduction

1. Records are kept because they serve as part of the memory of the organization. Records are not kept because of what they look like.
2. Records also serve as evidence and a way of showing what actions and decisions the organization made.
3. The legal definitions describe why and how we keep a special type of organizational memory.

Chapter 2 - Records Definitions and Regulations

1. Records: documentary material, regardless of physical form and characteristics, which contains information concerning the conduct of Federal business. Anything used to record the result of an action or decision that you make as part of your job is a record.
   a. All recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of data in them. See 44 U.S.C. 3301
   b. Books or records of account or minutes of proceedings of any department or agency of the United States shall be admissible to prove the act, transaction or occurrence as a memorandum of which the same were made or kept. See 28 U.S.C. 1733.
   c. Properly authenticated copies or transcripts of any books, records, papers or documents of any department or agency of the United States shall be admitted in evidence equally with the originals thereof. See 28 U.S.C. 1733.

d. If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any photographic, photostatic, microfilm, micro-card, miniature photographic, or other process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not and an enlargement or facsimile of such reproduction is likewise admissible in evidence if the original reproduction is in existence and available for inspection under direction of court. The introduction of a reproduced record, enlargement, or facsimile does not preclude admission of the original. This subsection 1 shall not be construed to exclude from evidence any document or copy thereof which is otherwise admissible under the rules of evidence. See 28 U.S.C. 1732.

2. Records include but are not limited to:
   a. Decision papers;
   b. Memoranda;
   c. Databases;
   d. Audio or video recordings;
   e. Publications;
   f. Web pages;
   g. Telephone logs; and
   h. Email messages.

3. Records are critical to the accountability of the Federal government and the agency; therefore, records must
   a. Act as part of the organizational memory: This means that the information must pertain to the organization and document an action or decision made on the behalf of the organization; and
   b. Have evidentiary value: The information must be in a form that can serve as legal evidence.

4. Data: Data describes a specific form of information. Data are sets of individual facts. For example, a piece of data about you is your first name. Data is most often kept in a database that groups related information. Central Index System2 (CIS2) is one of the most frequently used USCIS databases. People often assume data is not a record. It can be. Data simply describes how the information is kept. Whether or not data is a record depends on the function of the information.

5. Documentary materials: records that meet the conditions specified in 36 CFR 1222.10(b)(1), see 36 CFR 1222.12(b):

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.

6. Documents: Sometimes people confuse document and record. Document describes the appearance and format of information. Record describes a function of the information.

Documents	Data
Primarily text	Discrete pieces of information
Narrative or tabular	Organized in strictly prescribed format
Loosely prescribed form or format	Generally managed by database software

7. Electronic record: any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record under the Federal Records Act. The term includes both record content and associated metadata that the agency determines is required to meet agency business needs. See 36 CFR 1220.18.
8. The Freedom of Information Act (FOIA) and Privacy Act of 1974 (PA) deal with the right of the public and individuals to access records kept by the government. DHS has trained FOIA/PA specialists to handle the complex issues of what information DHS can and cannot release. For more information, see the following references:
   a. FOIA provides that any person has a right to request access to Federal agency records. See 5 U.SC 552.
   b. PA establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. See 5 U.S.C. 552a.
   c. For more information, see the USCIS FOIA/PA website.
9. Metadata: consists of preserved contextual information describing the history, tracking, and/or management of an electronic document. See 36 CFR 1220.18.
10. Nonrecord: Not all documents or data are records. See 36 CFR 1222.14.
    a. Nonrecord materials: U.S. Government-owned documentary materials that do not meet the conditions of records status (see 36 CFR 1222.12(b)) or that are specifically excluded from the statutory definition of records (see 44 U.S.C. 3301). An agency's records management program also needs to include managing nonrecord materials. There are three specific categories of materials excluded from the statutory definition of records:

i. Library and museum material (but only if such material is made or acquired and preserved solely for reference or exhibition purposes), including physical exhibits, artifacts, and other material objects lacking evidential value.
ii. Extra copies of documents (but only if the sole reason such copies are preserved is for convenience of reference).
iii. Stocks of publications and of processed documents. Catalogs, trade journals, and other publications that are received from other Government agencies, commercial firms, or private institutions and that require no action and are not part of a case on which action is taken. (Stocks do not include serial or record sets of agency publications and processed documents, including annual reports, brochures, pamphlets, books, handbooks, posters and maps.)

b. Some examples of nonrecord materials include:
   i. Routing slips that do not add anything other than routing information;
   ii. Blank forms; and
   iii. Computer printouts from agency systems that have no added annotations.

11. Official record versus unofficial record:
   a. The USCIS Official Record is material created or received as a result of official government action and is preserved because it contains evidence or information of value. An example of an "Official Record" is the existing paper A-file and the N-400 with supporting documents ingested into ELIS.
   b. In the interim ELIS N-400 process, the term "Unofficial Record" refers to the paper N-400 Drop File Packet temporarily stored in the paper A-file until the interview, adjudication, and ingestion into ELIS is complete.
   c. If the N-400 Drop File Packet is annotated during the adjudication process, the annotation is changed to this record and therefore must be scanned/ingested into ELIS as the official record.
   d. In general, the USCIS Unofficial Record is a copy of materials, documents, publications, standard government forms, and library material intended solely for reference or exhibition.
   e. To view more training material relating to official versus unofficial records as it pertains to the N-400 process, please click this training link. How to Handle N-400 Official and Unofficial Records - Video.

12. Permanent record: any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States, even while it remains in agency custody. Permanent records are those for which the disposition is permanent on SF-115, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973. The term also includes all records accessioned by NARA into the National Archives of the United States. See 36 CFR 1220.18.

13. Record Series or Series: A group of related files that have the same retention period and serve the same function. See 36 CFR 1220.18. Some examples of files series are:

a. A-files; and
b. Administrative correspondence files.

14. Recorded information: all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. See 44 U.S.C. 3301.
    a. Examples of "recorded information" includes but is not limited to
        i. Books,
        ii. Papers,
        iii. Maps,
        iv. Photographs,
        v. Machine readable materials,
        vi. Other documentary materials made, and
        vii. Is subject to the Archivist's determination.
    b. The Archivist's determination whether recorded information, regardless of whether it exists in physical, digital, or electronic form, is a record shall be binding on all Federal agencies.

15. Records Schedule or Schedule, see 36 CFR 1220.18:
    a. Form SF-115, Request for Records Disposition Authority, that has been approved by NARA to authorize the disposition of Federal records;
    b. A General Records Schedule (GRS) issued by NARA; or
    c. A published agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more SF-115s or issued by NARA in the GRS.

16. Retention period: the length of time that records must be kept. See 36 CFR 1220.18.

17. Temporary record: any Federal record that has been determined by the Archivist of the United States to have insufficient value (on the basis of current standards) to warrant its preservation by the National Archives and Records Administration. See 36 CFR 1220.18. This determination may take the form of:
    a. Records designated as disposable in an agency records disposition schedule approved by NARA SF-115; or
    b. Records designated as disposable in a General Records Schedule.

18. Unscheduled records: Federal records whose final disposition has not been approved by NARA on an SF-115. Such records must be treated as permanent until a final disposition is approved. See 36 CFR 1220.18.

19. Working files: preliminary drafts, rough notes, and other similar materials. 36 CFR 1222.12(c). Working files are records and must be maintained in a record file for purposes of adequate and proper documentation 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; and
b. They contain unique information, such as substantive annotations or comments included therein, that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.
c. **USCIS strongly discourages keeping any records in a working file or folder**. Within USCIS, **work folders** should have only copies of documents. Only the person who creates the work folder keeps it. If anyone else needs the information, then it is a record. Don't keep it in a work folder. File it appropriately.

Chapter 3 - Records Maintenance

1. Records versus nonrecords examples:

Records	Nonrecords
Information made or received under Federal law or when conducting agency business	Library materials
Information preserved as evidence or because of the information's value	Copies of publications
Copies of documents with comments and meaningful annotations	Extra copies without any substantial annotations
E-mail used to conduct agency business	Blank forms

2. Lifecycle of Records: Records lifecycle is a core concept in the field of records management. It is the idea that records go through several stages in life.
   a. This conceptual model describes three interrelated stages in the life of a record:
      i. Creation. Records are produced;
      ii. Maintenance and Use. Complete records are maintained; records can be located when needed; records, non-record materials, and personal papers are maintained separately; and the identification and retention of permanent records are facilitated; and
      iii. Disposition. Records are no longer needed to conduct current government business and are transferred or destroyed as dictated by the approved records schedule.
   b. During each stage of its life, the record has differing management needs and different levels of activity. The other important part of this concept is that most records have a defined life span.
3. Records continuum: The records continuum is a concept developed by the Australian Archives. It differs from the records lifecycle model in one crucial aspect. In this model, management of records begins before creation and continues throughout the entire life of the record. Pre-creation planning includes:

a. Choosing media that best suits the record and the needs of the organization for each stage of the records life; and
b. Planning for changes in media, accessibility, and usage patterns as the record ages.

4. Both models are useful because they emphasize the need for management of records especially:
   a. Analyzing how the organizations need for information from a record changes as the record ages; and
   b. Planning and investing in a record keeping process that takes into consideration the change in assets needed as the records age. Assets include storage space, equipment, and labor.

5. The content of the record, rather than the format (for example, memo, email, et cetera), determines how the record needs to be safeguarded.
   a. Classified records contain information impacting the security of the United States. Consult the USCIS Security Handbook or the chapter on handling classified records for more information.
   b. Sensitive records contain information that should not be released to the public. The Freedom of Information Act and Privacy Act (FOIA/PA) list examples of this type of information.
   c. Routine or non-sensitive information includes such things as:
      i. Copies of policies and procedures that do not reveal details of law enforcement activity, internal personnel matters, or that could be used for fraud;
      ii. Routine correspondence that does not contain information about individuals;
      iii. Printouts of broadcast emails; and
      iv. Copies of information printed off the Internet.
      v. If you are uncertain whether or not a record contains sensitive information, treat it as sensitive.

Part C - Record Keeping Responsibilities

Chapter 1 - Agency Responsibilities

1. The head of each Federal agency must make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. These records must be designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. See 44 U.S.C. 3101.

2. The head of each Federal agency must establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. See 44 U.S.C. 3102.

3. Agencies must create and maintain authentic, reliable, and usable records and ensure that they remain so for the length of their authorized retention period. See 36 CFR 1220.32. A comprehensive records management program provides policies and procedures for ensuring that:
   a. Records documenting agency business are created or captured;
   b. Records are organized and maintained to facilitate their use and ensure integrity throughout their authorized retention periods;
   c. Records are available when needed, where needed, and in a usable format to conduct agency business;
   d. Legal and regulatory requirements, relevant standards, and agency policies are followed;
   e. Records, regardless of format, are protected in a safe and secure environment and removal or destruction is carried out only as authorized in records schedules; and
   f. Continuity of operations is supported by a vital records program. See 36 CFR 1223.
4. Agency records management programs must provide for the following. See 36 CFR 1220.30.
   a. Effective controls over the creation, maintenance, and use of records in the conduct of current business; and
   b. Cooperation with the Archivist and the Administrator of GSA in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and destruction of records of temporary value. See NARA Bulletin 2014-04 Format Guidance for the Transfer of Permanent Electronic Records for regulations regarding formats.

Chapter 2 - Employee Responsibilities

1. All Federal employees are responsible for creating and helping to maintain full and adequate documentation for your job function. See 36 CFR 1220.30. If your answer to any of the following questions is "yes," you must create a record for full and adequate documentation.
   a. Does a statute, regulation, or Congress require making a record?
   b. Is your action creating or supporting a financial or legal claim or obligation by either the government or an individual?
   c. Are you taking an action, conducting a transaction, or making a decision on the behalf of Department of Homeland Security (DHS)?
   d. Does your job make you responsible for providing information that is required to operate a DHS program or to support any DHS function?
   e. Does your job make you responsible for providing information that makes it easier to take DHS actions and keep them consistent?
   f. Does your job make you responsible for providing information documents or helps implement decisions, policies, or directives?
   g. Are you recording minutes or notes from a board, committee, or staff meeting?

2. All Federal employees are responsible for
   a. Ensuring records are secure and handled properly;
   b. Reporting lost, destroyed, or damaged records to the Records Unit; and
   c. Following the approved NARA retention schedules when disposing of records. Failure to adhere to retention could lead to criminal penalties. The maximum penalty for the willful and unlawful destruction, damage, or alienation of Federal records is a $2,000 fine, 3 years in prison, or both. See 18 U.S.C. 2071.

3. All Federal employees are responsible for securing Personally Identifiable Information (PII).
   a. PII is defined as "any information that permits the identity of an individual to be directly or indirectly inferred," such as a social security number, birth-date, A-file number, etc. Breaches of PII's occur when this personal information is available to those without legitimate access or need for it.
   b. PII breaches include but are not limited to:
      i. Placing PII on thumb-drives/CDs/DVDs without proper encryption;
      ii. Leaving PII documents on a fax machine or copier; or
      iii. Improperly storing documents containing PII, or improperly discarding PII documents.
   c. Failure to follow legal authorities can result in civil or criminal penalties, reprimands, suspensions or employment terminations for showing a gross disregard or pattern of error in the safeguarding of PII. For more information on PII and safeguarding procedures, please see the memo titled USCIS Policy Regarding Personally Identifiable Information and the Office of Privacy Connect site.

4. All DHS employees are responsible for:
   a. Keeping track of the immigration records in your Responsible Party Code (RPC) and in your possession;
   b. Responding promptly to requests for immigration records in your RPC;
   c. Ensuring immigration records that cannot be released are marked as In-Use in RAILS; and
   d. Working with requesters to provide either the immigration record or the information needed to make an accurate and timely decision.

5. All Supervisors and Managers are responsible for:
   a. Ensuring individuals respond to record requests according to the required guidelines; and
   b. Following up on late responses.

Chapter 3 - Email Responsibilities

1. DHS email systems are for official use only by authorized personnel. The information in these systems is Departmental, not personal. Email is provided for official use, with limited personal use allowed. No expectation of privacy or confidentiality applies.

2. This guidance applies to all incoming and outgoing DHS email, including to or from non-DHS and outside sources, for example emails sent to a personal email address.

3. Email must be preserved for the appropriate retention period along with its essential transmission and receipt data (names of sender and addressee(s) and date the message was sent) in order for the context of the message to be understood.

4. The sender and the person who receives electronic mail determine independently whether the message and its attachments meet the definition of a Federal record for their office. See 44 U.S.C. 3301. The following are examples of email that constitute Federal records.
   a. Email that contains substantive information that is necessary to adequately and properly document the activities and functions of DHS;
   b. Email 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;
   c. Email that provides documentation of significant DHS decisions and commitments reached orally (person-to-person, by telecommunications, or in conference);
   d. Email that conveys information of value on important DHS activities, if the email message adds to a proper understanding of DHS operations and responsibilities;
   e. Email that documents the formulation and execution of basic policies and decisions;
   f. Email that documents important meetings;
   g. Email that denotes actions taken by DHS officials and their successors;
   h. Email that makes possible a scrutiny by the Congress or other duly authorized agencies of the Government; and
   i. Email that protects the financial, legal, and other rights of DHS and of persons directly affected by the Department's actions.

5. If an email 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 transitory.

6. Federal record emails may not be altered or improperly destroyed. This includes the email message itself along with the record of transmission, receipt date, and any attachments.

7. The retention period for Federal record email is governed by the appropriate NARA-approved DHS records control schedule or the General Records Schedule (GRS). Email users who are uncertain about the disposition of email messages should contact their program office Records Officer for assistance.

8. Email determined to be Federal records falls into three categories: permanent records, temporary records, and transitory records. If an email is an unscheduled record, it must be treated as permanent until NARA approves a schedule.
   a. Permanent emails are those messages that have sufficient value to warrant continued preservation by the Federal Government. These 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.

b. Temporary emails 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.
c. Transitory emails are those messages of short-term interest which have no documentary or evidential value and normally need not be kept more than 90 days.

9. Disposition of all email records will be made in accordance with an authorized records disposition schedule.
   a. When paper files are used as the recordkeeping system, permanent and temporary email are maintained and made available for office use by printing the email message (with attachment) and filing in the manual recordkeeping system.
   b. When the recordkeeping copy is maintained in paper, the printed email 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.
   c. When an electronic recordkeeping system is used, emails are filed electronically. This method requires the ability to perform preservation, protection, storage, retrieval, and disposition through the email application system itself; or copy email records into an electronic recordkeeping system, able to perform all the functional requirements of the Federal regulations. "Backups" made as a normal part of email systems operation and maintenance do not meet these requirements and should not serve as an electronic recordkeeping system.
   d. Email systems may also provide users with the ability to request acknowledgements or receipts showing that an email message reached the mailbox or inbox of addressee(s) and was accessed. Email 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 email message was received and accessed. In such instances, receipt data associated with the record copy of the email message will be preserved.

10. Additional guidance and definitions can be found in the DHS Records Management Handbook. Electronic Records Scheduling information can be found on the NARA website.

Chapter 4 - Establishing a File Control Office (FCO)

1. To request the establishment of an FCO, an office must submit:
   a. A signed memorandum, routed through their chain of command, to IIMD;
   b. A Data Change Request for assignment of a DHS Location Code; and
   c. A completed copy of the FCO Certification Checklist.

2. The directorate requesting the establishment of an FCO is responsible for determining the appropriate level within the chain of command for this approval.

3. The memo must include the following information:
   a. New office location, including sub offices or addresses of separate buildings within the FCO;

b. Copies of training certificates for records employees at the new FCO in the following subject areas:
   i. Records Management;
   ii. RAILS;
   iii. CIS2;
   iv. Basic Records; and
   v. Records Assurance.

   If not available at the time of the request, the FCO must submit certificates within 30 days of FCO establishment;
c. Names of local ICE and CBP points of contact (POCs) who can address all Records issues at the FCO;
d. Prospective establishment date;
e. Names of RAILS Administrator; and
f. FCO Records POC and email box.

4. Each FCO or Records group must have an email box specifically for Records matters.
   a. These email boxes must not be used for expedited requests.
   b. The email address must be the three digit FCO followed by the letters REC. For example, the email address for Los Angeles is LOSREC and the email address for Miami is MIAREC.
   c. The only exception is the NRC, which has a number of email accounts for different services. Email addresses for the NRC are located in the NRC Customer Guide.
5. FCOs must have sufficient number of Records staff to process all records-related tasks.
6. The FCO is responsible for purchasing all equipment needed for records management to include:
   a. Audit guns;
   b. Barcode scanners;
   c. Specialized barcode printers; and
   d. Any other necessary equipment.
7. After approvals are obtained, IIMD will:
   a. Notify the appropriate headquarters offices when the new FCO is active in RAILS and CIS2; and
   b. Coordinate with the requesting office and any other affected offices to ensure current records physically at the FCO are in RAILS and CIS2. IIMD staff will work with each office on an individual basis to ensure a smooth transition.

Chapter 5 - FCO Responsibilities

1. A File Control Office (FCO) is an office that is authorized to manage immigration records, such as A-files and Receipt files. FCOs can create, store, transfer, receive, maintain, and retire immigration records. Previously, some offices were referred to as Case Control Offices (CCO), but with the implementation of RAILS all offices are referred to as FCOs.

2. FCOs are responsible for
   a. All records in its jurisdiction to include sub-offices, field offices, ports of entry, and border patrol stations within the surrounding area;
   b. Record retirements, mandatory annual audits of records, record creation, consolidation, and de-consolidation;
   c. Managing all record tracking and control reports;
   d. Coordinating with the Mail Management Division to establish mail procedures;
   e. Developing Continuity of Operations Planning, see RPM Volume 6;
   f. Coordinating with ICE and CBP per the Service Level Agreement (SLA); and
   g. Adhering to USCIS records policies and procedures as codified in the RPM.
3. FCOs must have access to all electronic systems that support records functions (such as, RAILS, CIS2, EDMS, and SMART). For more information on systems, see RPM Volume 4.
4. FCOs are the only offices permitted to transfer records in and out of external offices. RAILS users can directly transfer records to other FCOs.

Chapter 6 - Records Custodian Responsibilities

1. Each FCO must designate a primary and an alternate Records Custodian with responsibility for file reviews. The primary role of the custodian is to safeguard the records which are created, used, and maintained for USCIS purposes while cooperating with other agencies where possible.
2. Each Records Custodian must know what can be disclosed and must exercise discretion whether to make such disclosures.
3. Records custodians will, upon request, provide agencies in their jurisdiction of the name, title, telephone number, and e-mail address of the designated Records Custodians.

Chapter 7 - Closing or Changing Jurisdiction of an FCO

1. IIMD requires at least 30 days advance notice before an FCO may cease operations. Once an FCO closes, the FCO that assumed the responsibilities of the closing FCO will manage all responsibilities, including record movement.
2. Before an FCO is closed or jurisdiction is changed, the requesting FCO must:
   a. Notify headquarters program offices; and
   b. Work with affected offices to ensure RAILS and CIS2 account for current records at the FCO.
3. To request to close or change the jurisdiction of an FCO, an office must provide IIMD with the following:

a. A signed memorandum notifying IIMD of the closure or change of jurisdiction, routed through the FCO's directorate. The directorate requesting the closure or change of jurisdiction of an FCO is responsible for determining the appropriate level within the chain of command for this notification;
b. A completed copy of the FCO Closing/Changing Certification Checklist;
c. A copy of the memorandum from USCIS to ICE and CBP explaining that the office is closing and referring ICE and CBP to another FCO; and
d. A list of all reports that the FCO will need to reconcile, including reports from SMART. IIMD will work with the FCO to reconcile all reports.

4. The FCO requesting to close or change jurisdiction must wait until the RAILS and CIS2 development teams can assist in electronically moving their records into the FCO that will have jurisdiction over the records.
   a. The new office that will have jurisdiction over the records will submit a name (usually the records manager) and a comment to the RAILS development team to associate with the record movement.
   b. The new FCO that will have jurisdiction over the records must also ensure that any missing or lost records are also moved into an RPC within the new FCO.
   c. RAILS and CIS2 development teams will inactivate or change the FCO code from the DHS Standard Tables.

5. Once the parties involved have physically moved all records to the new FCO assuming jurisdiction over the records, the new FCO must perform a physical audit to account for all records.

Part D - Retention and Disposition of Records

Chapter 1 - Retention and Disposition of Records Regulations

1. Federal law regulates how long records are kept and what is the final disposition of (or what will ultimately happen to) the records.

2. 36 CFR 1224.10 In order to properly implement the provisions of §§1220.30(c)(2), 1220.32(e), and 1220.34(c), (f), and (g) of this subchapter agencies must:
   a. Ensure that all records are scheduled in accordance with part 1225 of this subchapter, schedules are implemented in accordance with part 1226 of this subchapter, and permanent records are transferred to the National Archives of the United States.
   b. Promptly disseminate and implement NARA-approved agency schedules and additions and changes to the General Records Schedules (GRS) in accordance with §1226.12(a) of this subchapter.
   c. Regularly review agency-generated schedules, and, if necessary, update them.
   d. Incorporate records retention and disposition functionality during the design, development, and implementation of new or revised recordkeeping systems (whether paper or electronic). See §1236.6 of this subchapter.

e. Provide training and guidance to all employees on agency records disposition requirements and procedures and other significant aspects of the records disposition program. When a new or revised records schedule is issued, provide specific guidance to employees responsible for applying the schedule.

3. 36 CFR 1225.10 All Federal records, including those created or maintained for the Government by a contractor, must be covered by a NARA-approved agency disposition authority, SF-115, Request for Records Disposition Authority, or the NARA General Records Schedules.

4. 36 CFR 1220 Subpart B outlines the regulations controlling records disposition and retention.
   a. Agencies must ensure the proper, authorized disposition of their records, regardless of format or medium, so that permanent records are preserved and temporary records no longer of use to an agency are promptly deleted or disposed of in accordance with the approved records schedule when their required retention period expires. As an intermediate step when records are not needed for current day-to-day reference, they may be transferred to a records storage facility.
   b. Agencies must secure National Archives and Records Administration (NARA) approval of a records schedule or apply the appropriate General Records Schedule (GRS) item before destroying any temporary records or transferring permanent records to the National Archives of the United States.
   c. Records must be destroyed based on the disposition stipulated in the retention schedule – not sooner, not later - unless prior written approval has been obtained from NARA.

Chapter 2 - Retention of Records

1. All Federal records must be scheduled either by an agency schedule or a GRS. See 44 U.S.C. 3303.

2. A retention schedule outlines:
   a. How long the agency keeps records?
   b. When the agency will transfer records to offsite storage?
   c. What will ultimately happen to the records?

3. The retention schedule is for the primary application and all supporting documentation. For example,
   a. Form DS-2019, Certificate of Eligibility for Exchange Visitor Status, is presented as support for Form I-539, Application To Extend/Change Nonimmigrant Status. Use the retention schedule for the I-539.
   b. A DS-2019 supports a Form I-485, Application to Register Permanent Residence or Adjust Status, the DS-2019 goes in the A-file as supporting documentation for the I-485.
   c. A DS-2019 by itself, use the retention for the DS-2019.

4. Do not intermingle applications/petitions having different retention periods in the same folder, unless they support a primary application.

5. There are two schedules:
   a. The NARA GRS provides mandatory disposal authorization for temporary administrative records common to several or all agencies of the Federal Government. They are issued by the Archivist of the United States under the authority of 44 U.S.C. 3303.
   b. USCIS Agency Retention Schedules may be found on the Records Officer Connect page under All Retention Schedules.
6. Unscheduled records are those not included on an agency schedule or on a GRS. Unscheduled records cannot be legally destroyed until a disposition has been approved by NARA using an SF-115, Request for Records Disposition Authority. Report any unscheduled records to your Records Supervisor, Regional Records Office or to the IIMD Records Officer for scheduling.

Chapter 3 - IRIS Quality Assurance / Quality Control for Scanning Records

1. Materials scanned into a USCIS electronic repository (ELIS, EDMS, or STACKS) must follow IRIS approved Quality Assurance / Quality Control (QA/QC) process. If you wish to deviate from the approved process, you must submit a request through the RPM mailbox requesting a deviation be authorized.
2. Records must be preserved according to the NARA Bulletin 2014-04 Format Guidance for the Transfer of Permanent Electronic Records.
3. User must select an applicable document type from the drop-down menu when uploading a document.
4. Prior to scanning, the scanner should be clean and free of dust, smears, or similar obstructions that might diminish the quality of the scanned image.
5. File size of ingested image cannot exceed 6MB per document.
6. Scans must be saved as a .PDF or .JPG.
7. If a document arrives in an envelope, both the contents and the envelope must be scanned.
8. Staples, paper clips, or other fasteners must be removed prior to scanning.
9. Pages must not be stuck together, crumpled or folded.
10. Blank pages must be removed.
11. If any text, image, marking, or other information appears on either side of the document, that side must be scanned. Each scanned page must be enumerated.
12. When scanning is complete, you must compare the digital images against the paper documents that were scanned in. If there are missing pages, illegible pages, incorrectly oriented pages, partially scanned pages, or any other deficiency that would impede the use of the digitized copy for any purpose the original paper document would have been used, you must delete the deficient copy and scan the document(s) again.

Chapter 4 - Disposition of Records

1. Disposition is the final step for a record. It is either destroyed or sent to NARA for accession into their permanent records. The disposition for most records is destruction or deletion.
2. Accessioning is the process of transferring physical and legal custody of permanent records from Federal agencies to NARA. Federal agencies are required to accession their permanent records into the National Archives. See 36 CFR 1235.
3. NARA uses the term temporary for records that will eventually be destroyed. A temporary record can have a very long life but still be considered a temporary record. Temporary records can be transferred to agency storage facilities or a Federal Records Center (FRC) nearest to the office location. See FRC locations.
4. NARA uses the term permanent for records that will be accessioned and kept forever.

Chapter 5 - Retirement of Records

1. Overview
   a. This section provides Federal records guidance on retiring agency records other than A-files (for example, program files, correspondence, financial records, et cetera) covered by approved disposition authorities.
   b. Records should be retired when they are no longer needed to conduct day-to-day operations.
   c. Records retirement is based on the disposition specified in the General Records Schedule (GRS) and is located on NARA's website or USCIS Records Officer Connect site where agency records schedules are located.
   d. Records are classified as either temporary or permanent.
2. The process of transferring records to offsite storage is called retirement. When USCIS retires a record, it is sent to a Federal Records Center (FRC). NARA runs several Records Centers across the United States. USCIS maintains control over its retired records.
3. USCIS has a contractual arrangement with NARA to store retired records.
4. At some point, USCIS transfers permanent records to NARA's custody. NARA keeps permanent records in the National Archives. Unlike records we have retired, NARA controls the permanent records transferred to them and unless there are security or privacy concerns, these records are open to the public.
5. Definitions commonly used in the retirement of records:
   a. Contingent Records: Records scheduled for final disposition at some unspecified future time after the occurrence of a particular event, such as the decommissioning of a vessel, the sale of property, or the destruction of a building.
   b. Frozen Records:Temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an investigation, require a temporary extension of the approved retention period.

c. Mixed Records: Records with different disposition authorities.
d. Non-paper Based Records: Records that are not made from paper materials including items such as videos, tape recordings, film, magnetic media, et cetera.
e. Permanent Records: Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes.
f. Temporary Records: Records approved by NARA for disposal, either immediately or after a specified retention period.
g. Unscheduled Records: Records whose final disposition has not been approved by NARA.

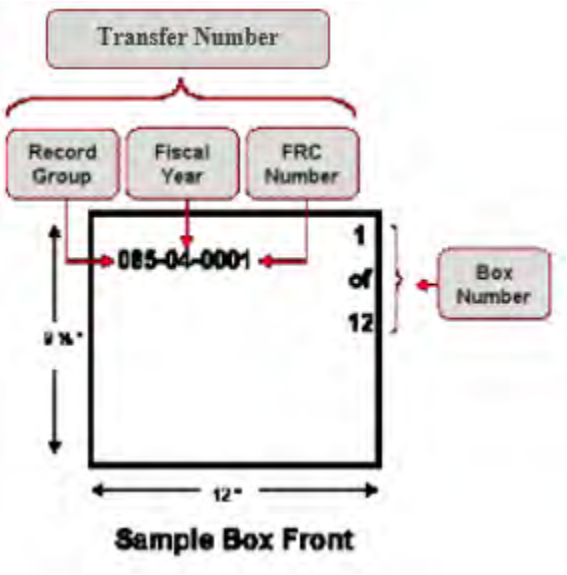
6. Shipping records to an FRC
   a. Shipments arriving at the FRC out of order, in oversize boxes, improperly taped or marked may require increased costs to the shipping agency.
   b. More detailed information is available on the NARA website regarding Shipping of Records and proper placement of boxes on pallets when required, see FRC toolkit for guidance.

7. Shipping contingent, frozen, mixed, non-paper based, permanent, or unscheduled records to an FRC, see flow chart:
   a. Arrangements must be made to ship the records to the appropriate FRC;
      i. To select the FRC closest to your office location, see listing of FRCs on the NARA website.
      ii. The FRC does not impose a limit on the number of boxes in a transfer.
   b. ARCIS must be checked to verify the transfer has been approved;
      i. If you are not currently an ARCIS user, see USCIS Records Officer Connect site for the ARCIS new user authorization form.
      ii. Submit completed form to arcishelp@uscis.dhs.gov.
   c. Once the transfer has been approved, an electronic Form SF-135, Records Transmittal and Receipt, and Box List of the records for each transfer must be submitted in ARCIS as well as a hard-copy placed in the front of both the first and last box of the shipment.
      i. Once you log into ARCIS, select Records Transfers.
      ii. Select Create Records Transfer. ARCIS will generate the Transfer Number after the Transfer is saved for the first time.
      iii. Complete the SF-135.
      iv. When selecting an Agency Contact, select a person who knows about the records and is responsible for answering questions.
      v. When selecting Agency Approver, select a person who is responsible for approving the transfer.
      vi. The Agency Official is the person who authorizes the transfer of the records. The Agency Approver and Agency Official may be the same person.
      vii. To attach a Box List, select Attachments and upload Box List.
      viii. When the SF-135 form is complete, select Submit to Approver.

d. Records must be shipped within 90 days of the approved transfer. Some centers will pick up agency records. Check with your local FRC for scheduling and fee information to determine the most economical approach. Additional guidance can be found in:
   i. The Mail Management Division USCIS Connect website;
   ii. Memo: Alternate Method of Shipping Files; and
   iii. Memo: Shipment of Large Volume Records.

8. Offices must use the following materials available through the current GSA Supply Catalog for preparing record transfers:
   a. Standard size record box (14 ¾" x12" x9 ½") for legal or letter size files, stock number: NSN 8115-00-117-8249;
   b. Clear packing tape (does not obscure numbers); and
   c. Felt-tip markers.

9. Requirements for boxing records for transfer to an FRC:
   a. Clear records must be retired in a series;
   b. Each series must be transferred separately;
   c. Packed boxes must have at least 1 to 2 inches of space to allow ease of records retrieval;
   d. Each box must be completely full;
   e. Letter-size files must face towards the front of the box;
   f. Legal-sized files must face toward the left side of the box;
   g. The outside of the box must be annotated in black felt-tip marker with numbers at least 1 ½ inches high as follows:
      i. Physical (PT) Number in the upper-left corner of each box, for example, 566-18-1234;
      ii. Box Number and total number of boxes in the accession in the upper right corner, for example 2 of 10;
   h. Boxes must not have labels or tape, unless shipping by commercial carrier or UPS.
   i. Transfer Number or agency box number must not be covered with tape.



Sample Box Front

10. Permanent records stored at the FRC are physically transferred into the custody of National Archives. When permanent records are eligible for transfer, the transferring official, usually the agency Records Officer, creates the transfer request in the Electronic Records Archives (ERA) system and submits it to NARA for approval.

11. Requests for records located at an FRC must be submitted through ARCIS, not an OF-11, Reference Request.
    a. When logging into ARCIS, initiate a reference request by selecting Reference Requests, then select CREATE.
    b. Proceed to initiate your request in ARCIS.
    c. Emergency situations or expedited requests may require same day pick-up by the requestor, using overnight express, commercial courier, or messenger (for example, court cases, terrorist threats, et cetera).
    d. Messengers must provide an official government photo ID and agency affiliation when arriving at the FRC to pick up requested files.

12. Records obtained from the FRC must be returned to the FRC for refiling when no longer needed.
    a. "REFILE" must be written on the cover letter; and
    b. The order of records within a file or the order of the files within a box must not be changed.

Chapter 6 - Destruction of Records

1. NARA handles destruction of records that have been retired to an FRC.

2. IIMD has the authority delegated from NARA to destroy records according to an approved disposition schedule. See 36 CFR 1226.24. This authority is delegated to local records supervisors.

3. If the records are to be destroyed in a USCIS office, you must
   a. Check the disposition schedule when screening documents for destruction;
   b. Not destroy documents set aside for destruction until a person trained in USCIS disposition procedures has reviewed them;
   c. Not destroy records required for an ongoing investigation or litigation;
   d. Destroy USCIS Limited Official Use documents by tearing or altering beyond recognition and reconstruction before disposing of them with other waste materials;
   e. Shred, pulp, pulverize, or burn Classified, Top Secret, Secret, and Confidential documents to 1/8 inch;
   f. Have two people present during the destruction process; and
   g. Keep a log of all locally destroyed records. See attached Excel spreadsheet for an example. Logs must contain the following:
      i. GRS Number (chapter and item) or the Department Disposal Authority Number;
      ii. Inclusive dates of the records;
      iii. Quantity in linear feet (this is the length of the shelf required to store the records);
      iv. Brief identifying information, varies with the type of records. For example. Information might include a range of numbers or indicate which office originated the records. Provide the best identifying information available;
      v. The date of destruction;
      vi. The printed name and signature of records supervisor authorizing the destruction;
      vii. Printed name and signature of both witnesses; and
      viii. Method of destruction.
   h. Apply the GRS 4.1: Records Management Records for the log.

4. Physical destruction can be contracted out. However, if the files are subject to the Privacy Act, a USCIS employee must stay with the records while they are in the custody of the contractor and witness the destruction.

5. The FRC must have agency approval before destroying records.
   a. Temporary records that have been retired to an FRC will be destroyed by NARA according to the destruction date specified on the SF-135.
   b. NARA electronically submits the Form NA 13001, Notice of Eligibility for Disposal, in ARCIS to the Agency Records Officer.
   c. An agency approved NA 3001 or a signed statement authorizing the destruction of the records must be returned to the FRC before the records can be destroyed.
   d. If the agency does not comply with specified rules, the FRC will have to retain the files resulting in the agency continuing to pay storage fees.

e. If the agency does not concur with the disposal, a justification for non-concurrence must be provided to the appropriate FRC.

Chapter 7 - Unauthorized Destruction or Removal of Records - Penalties and Reporting

1. Penalties for not following retention schedules or for unlawful or accidental removal, defacing, alteration, or destruction of records or the attempt to do so include a fine, imprisonment, or both. See 36 CFR 1230.12.
2. The maximum penalty for stealing, converting to someone else's use, selling, conveying, or disposing of any record is $10,000 in fines or ten years imprisonment. See 18 U.S.C. 641.
3. The maximum penalty for concealing, removing, mutilating, or destroying; attempts to do so; or intends to do so to any record is $2,000 in fines or three years imprisonment. See 18 U.S.C. 2071.
4. Retention schedules apply to all records, including electronic records and email. Erasing electronic records does not destroy them. See NARA's General Records Schedules 3.1, 3.2, 4.1, and 4.3 and Email Management.
5. Federal agencies are required to report promptly any unlawful or accidental destruction, disclosure, defacing, alteration, or removal of records in the custody of that agency to NARA
   a. By mail
      National Archives and Records Administration
      Office of the Chief Records Officer (AC)
      8601 Adelphi Rd.,
      College Park, MD 20740-6001
   b. Or email RM.Communications@nara.gov
   c. The report must include:
      i. A complete description of the records with volume and dates if known;
      ii. The office maintaining the records;
      iii. A statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records;
      iv. A statement of the safeguards established to prevent further loss of documentation; and
      v. When appropriate, details of the actions taken to salvage, retrieve, or reconstruct the records.
   d. The report must be submitted or approved by the individual authorized to sign records schedules as described in §1220.34(b) of this subchapter. See 36 CFR 1230.14
6. This report has been cleared in accordance with GSA regulations in 41 CFR and assigned Interagency Report Control Number 0285 - NAR-AR.
7. The Archivist of the United States will assist the head of the agency in contacting the Attorney General for the recovery of any unlawfully removed records.

8. If you become aware of unlawful or accidental destruction, defacing, alteration, disclosure or removal of records, report it to your Records Supervisor, Regional Records Office, or IIMD immediately. You will be entitled to whistle blower protection, if needed.
9. Do not send reports directly to NARA. Reports should be sent to IIMD, Policy and Analysis Branch (PAB) who will coordinate reporting to NARA.

Volume 2 - Reserved

Volume 3 - Immigration Records

Part A - Immigration Records Basics

Chapter 1 - Immigration Record Basics

1. DHS is responsible for several types and classifications of immigration records that deal with individuals who apply for a benefit or have an enforcement or other action as prescribed by the INA.
2. Immigration records are generally typed by their length of value and disposition; characterized by their physical or electronic state; and classified by the sensitivity of the information contained within the record.
3. If required, an individual is assigned an A-number. Otherwise, individuals with immigration records are searched or referred to by name and/or date of birth or receipt number.
4. An A-number (A#) is a unique identifier assigned by U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), or Department of State (DOS) to individuals who apply for an immigration benefit, have a pending enforcement action, or have other actions prescribed by the INA and other regulatory guidelines. For examples of when an A-file would be created, refer to RPM Vol 3, Part A, Chapter 2.
5. An A# must
   a. Start with an "A" and contain nine (9) numeric digits. If necessary, leading zeros must be added to ensure the total number of digits is nine, for example A023456789;
   b. Not contain special characters, spaces, prefixes, or alpha characters (other than the leading "A").
   c. For IT systems display and interface exchanges, an A# is the nine numeric characters, 000000000, without the leading "A." In the record layout for interface exchanges, only nine numeric characters are sent in the position identified for the A# in the record layout. For example, the record layout may contain 200 characters, but the A# is always provided in positions 1–9 in the update record.
6. Prior to March 2006, specific A# series were assigned to designated programs. Programs may now use available numbers as needed. Identity and Information Management Division (IIMD) manages issuance of A# that will be printed as needed from a block or blocks of assigned numbers. The "Table of Assigned A-numbers" in SMART provides historical information on previous A# designations. This table is available under the RTEM dashboard—A-NUM MGMT tab—A-number ranges (RAILS-ODS) report.
7. Exceptions to the statement above are Visa A#'s reserved for the Department of State (30,000,000 to 69,999.999) and Employment Authorization Documents (100,000,000 to 199,999,999).

8. Contact RPM@uscis.dhs.gov if you have questions concerning A# assignments.

Chapter 2 - Types of Immigration Records

1. Alien records (A-files)
   a. A-files are records maintained on an individual that documents the history of interaction with USCIS, ICE, and CBP as prescribed by the Immigration and Nationality Act (INA) and other regulations regarding immigration benefits.
   b. A-files contain forms, correspondence, biometrics, etcetera to support the decision to grant or deny immigration-related benefits and provide information that may be used in enforcement actions.
   c. A-files may exist in physical or digital format in EDMS, ELIS, or STACKS.
   d. A-files are created when an application or petition for long-term or permanent benefit is received or in relation to pending enforcement action. The list below is not comprehensive and is presented to provide examples of people who would receive an A-number:
      i. People with immigrant status;
      ii. People who break immigration laws;
      iii. People who have derived or acquired citizenship;
      iv. Asylees and refugees; and
      v. Native-born citizens who have expatriated.
   e. A-files are not created when
      i. Another A-number exists for an individual; or
      ii. Source documents originate outside of DHS as they are not part of the permanent record, for example: documents issued by other Federal agencies, State or local criminal records, and personal original documents submitted by applicants.
   f. A-files are permanent records that will be retired. See RPM Vol 3, Part G.
      i. When the retention period is met, the files will be released to the custody of the NARA, at which time the information may become available to the public.
      ii. For individuals born less than 100 years ago, A-files are stored and owned by DHS.
      iii. For individuals born 100 years ago or more, A-files are stored and owned by NARA.
      iv. Only non-classified A-files go to the Lee's Summit FRC.

2. Temporary alien records (T-files)
   a. T-files contain documents required for long-term or permanent immigration benefits or enforcement actions that would trigger creation of an A-file.
   b. T-files exist in physical format.
   c. When the action required to create the T-file is complete, the FCO that created the T-file must consolidate it into the corresponding A-file. Exceptions:
      i. If the corresponding A-file is at the NRC, send T-file to NRC for consolidation.
      ii. If the corresponding A-file is digitized, send T-file to NRC for retirement.

d. T-files are created by an FCO to store permanent documentation when the original A-file cannot be found immediately or while waiting for the A-file to arrive from another FCO.
e. T-files are not created if there is no corresponding A-file or Sub-file.

3. Substitute alien records (Sub-files)
   a. Substitute A-files, also referred to as Sub-files or S-files, replace the original A-file when an A-file is missing or lost:
      i. More than 60 working days,
      ii. After a special search has been conducted, and
      iii. After the missing or lost procedures have been followed; or
      iv. When the A-file has been destroyed.
   b. Sub-files exist in physical format.
   c. The office with the business need for the record is responsible for creating the Sub-file.
   d. Sub-files cannot be created because an FCO does not respond to your request for the record, does not release the record, and/or continues to place the record *In Use* in RAILS.
   e. If the corresponding A-file is found, the FCO that created the Sub-file must consolidate the Sub-file into the A-file. Otherwise, the Sub-file is a permanent record that is eventually retired by the NRC.

4. Receipt records (Receipt files)
   a. Receipt files, most commonly used for non-immigrant forms, have temporary value.
   b. Receipt files deemed to have permanent value are consolidated into A-files.
   c. Digitized Receipt files are electronic images of physical applications processed by Lockbox Operations facilities managed by the USCIS Office of Intake and Document Production (OIDP) and stored in the EDMS Digitized Receipt files.
   d. The Digitized Receipt files stored in EDMS are not considered the official Agency record of the Receipt file. The paper file is the official record for the Agency.
   e. Receipt files are destroyed per retention schedules.
   f. The retention period for the digitized content stored in the EDMS Receipt file partition has a different retention period from that of the physical Receipt file. Each Receipt file is a single PDF and includes the application and supporting documentation.
   g. Digitized Receipt files are retained for 1 year for accepted applications and 6 years for rejected applications.
   h. NOTE: If required, a Records Administrator can place a "hold" on the retention expiration.

5. Alpha files
   a. Alpha files contain the same types of forms as Receipt files but are not A-file material. Receipt files contain forms sent to a Service Center; whereas, Alpha files are forms received in all other DHS offices.
   b. Alpha files are kept in the office that creates the record.
   c. Folders must be arranged by form type and year.

i. The front of each set of folders for a particular form and year must have the following information:
   - Form number and complete name;
   - Disposal Authority Number or General Records Schedule Number;
   - Year form was adjudicated;
   - Date of retirement (if applicable); and
   - Date of destruction.

ii. Subsequent labels in the folder, must contain the form type and the year and month the form was adjudicated.

iii. For example:

I-765 Application for Employment Authorization **N1-85-94-2 2002** **Retire to FRC Jan. 2005** **Destroy Jan. 2010**
I-765 2002 **January**
I-765 2002 **February**

d. Arranging folder contents

i. File documents in alpha files in a way that balances the ease of filing with the ability to find the documents. You can arrange documents in alphabetical, chronological, numerical, or terminal digit order.

ii. Keep your filing arrangement simple.
   - Use your file folders to denote groups of forms; and
   - Do not arrange individual documents within the folder in any order other than reverse chronological order (newest in the front).

e. Folders must be kept in your office for the length of time specified by the disposition schedule. Then retire to the FRC or destroy as specified.

6. Work files (W-files)

a. W-files are temporary files that contain notes or copies.

b. W-files are owned and stored by the person who created the file and should not be entered into RAILS.

c. W-files are created when an officer needs to create notes or make copies of documents that would not be part of the official record.

d. W-files must not contain A-file material. If A-file material exists in a W-file, it must be consolidated into the A-file. If the A-file has been digitized, the W-file must be converted to a T-file and the material sent to the NRC for scanning as interfiling upon completion of use.

e. Upon completion of the need for the W-file, the file must be destroyed in accordance with USCIS privacy policies and practices.

7. Historical Records
USCIS identifies two types of "historical records":
   a. Records identified by the Archivist of the United States for permanent retention due to their historical value, based on the Records Act, including old records already transferred to National Archives custody, as well as current records scheduled as permanent.
   b. Historical records are files, forms, and documents now located within the following records series, see 8 CFR 103.39:
      i. Naturalization Certificate files (C-files) are series records relating to all U.S. naturalizations in Federal, State, county, or municipal courts, overseas military naturalizations, replacement of old law naturalization certificates, and the issuance of Certificates of Citizenship in derivative, repatriation, and resumption cases used from September 27, 1906 to April 1, 1956. People naturalized before April 1, 1956 were assigned a C-file. People naturalized on or after April 1, 1956, were assigned an A-file. A-files were consolidated into C-files created before 1956, but the C-file continues to be the official record.
      ii. Microfilmed Alien Registration Forms, from August 1, 1940 to March 31, 1944. Microfilmed copies of 5.5 million Alien Registration Forms (Form AR-2) completed by all aliens age 14 and older, residing in or entering the United States between August 1, 1940 and March 31, 1944.
      iii. Visa files, from July 1, 1924 to March 31, 1944. Original arrival records of immigrants admitted for permanent residence under provisions of the Immigration Act of 1924.
      iv. Registry files, from March 2, 1929 to March 31, 1944. Original records documenting the creation of immigrant arrival records for persons who entered the United States prior to July 1, 1924 and for whom no arrival record could later be found.
      v. Alien files numbered below 8 million (A8000000) and documents therein dated prior to May 1, 1951. Individual alien case files (A-files) became the official file for all immigration records created or consolidated after April 1, 1944.
      vi. Note: C-files remained the official case file for any subject who naturalized or was issued a certificate between April 1, 1944 and March 31, 1956.
   c. Most historical records are in the custody of IIMD or in USCIS custody at an FRC.
   d. The USCIS Genealogy Program has published general descriptions of the agency's historical records as defined in 8 CFR 103.39.

8. Vessel arrival and departure records

a. Form I-418, Passenger List - Crew List, documents crew arrival by water at any port within the United States from any place outside the United States. The Manifest provides a complete list containing the names of all aliens employed on the vessel, the positions they hold in the crew, when and where they were shipped or engaged, and those to be lawfully paid off or discharged in the port of arrival.
b. Effective February 11, 2008 in accordance with a muster "Storage of Arrival/Departure Crew Manifest (I-418)" distributed by CBP, Admissibility and Passenger Programs, Office of Field Operations; CBP will no longer send matched arrival and departure crew manifests (I-418) to the NRC for storage. The CBP port of arrival will house the matched documents for 6 months, and then forward them to the local FRC for maintenance and storage.
c. For questions or concerns regarding this matter, contact the CBP Admissibility and Passenger Program at ENFORCEMENTPROGRAMSDIVISION@cbp.dhs.gov.

Chapter 3 - Characteristics of Immigration Records

Immigration records bear one of the following four basic characteristics:

1. Physical - records stored only in physical form and have no corresponding digitized or electronic content in any electronic systems.

2. Digitized – records that have been scanned and captured in either the Electronic Document Management System (EDMS) for A-files, EDMS Receipts, or STACKS.
   a. RAILS and CIS2 indicate the digitization of a record with "DIG" or "DIGITIZED FILE – VIEW THE FILE IN EDMS"
   b. The digitized record is representative of all documents contained in the physical A-file. If there is material within the record that cannot be digitized (for example, newspaper(s), magazine(s), book(s), audio and/or video cassette(s), catalog(s), CD-ROM(s), and/or sealed envelopes) the digitized image is annotated by a document indicating *Unscanned Items*.
   c. Digitized records should not be printed. If a printout is created, it must be placed in a W-file. If a change/remark is made to the printout or new material is added to the W-file, the file should be converted to a T-file and sent to the NRC for scanning as interfiling upon completion.
   d. For more information on digitized records, see the NRC Customer Service Guide.
   e. Receipt files are not electronically combined after the Receipt file has been physically combined with the A-file and the A-file has been digitized.
   f. To request a correction to a digitized record, such as a duplication of A-number assignment, email the request to: edmssupport@uscis.dhs.gov with the subject: Correction to Digitized Record. The email should include:
      i. Request for a correction to a digitized record in EDMS;
      ii. A-file number and the information that needs to be corrected; and
      iii. Name, telephone number, office, and email address of the person requesting the change.

iv. NOTE: Supporting documentation to verify the requested change may be requested in order to prevent fraud and to ensure the integrity of the record.

g. To consolidate files that have been digitized,
   i. send a request to the NRC, SODA Team mailbox, SODATEAM.NRC@uscis.dhs.gov;
   ii. The subject line should state: Request for File Consolidation;
   iii. The body of the email message must include the following:
      - A-numbers to be consolidated;
      - Name/Location of the requester (Agency/FCO or Sub-Office Code);
      - Telephone and Fax number of the requester;
      - Email address of the requester; and
      - Reason for the Request to include designation of Primary/Secondary.

3. Electronic – records stored only in electronic form and have no corresponding physical records.

4. Hybrid – records that can contain content in physical, digitized, and/or electronic form.
   a. You must search RAILS to ensure all documentation and corresponding records are found.
   b. Digitized-Physical examples:
      i. A-file was not available or could not be located at the time of adjudication, so a T-file was created. If the files were not consolidated prior to digitization, the T-file will remain in a physical state while the original A-file will be digitized.
      ii. A-file contains classified document. The classified document would be stored in a physical A-file, while the remaining documentation would be stored in digitized form.
   c. Electronic-Physical examples:
      i. Physical A-file exists for Form I-130, Petition for Alien Relative, and Form I-485, Application to Register Permanent Residence or Adjust Status, and Form N-400, Application for Naturalization is in ELIS
      ii. Physical A-file exists for I-213, Record of Deportable / Inadmissible Alien, and Form N-600, Application for Certificate of Citizenship, is in ELIS
   d. Digitized-Electronic-Physical example:
      i. Form I-130 has been digitized and is available in EDMS,
      ii. Form I-485 is in ELIS, and
      iii. Form I-290b, Notice of Appeal or Motion, is in physical form.

Chapter 4 - Classification of Immigration Records

1. Immigration records are unclassified unless National Security Information (NSI) is introduced into the record, even if the classified information is limited to a single document. See USCIS Office of Security & Integrity Security Handbook Chapter 8 Classified National Security Information (USCIS Security Handbook Chapter 8).

2. When classified information is introduced into a record, the entire record must be marked as classified.
3. All USCIS Federal and contract employees authorized to use or handle classified material are responsible for handling and safeguarding any classified records assigned to them in accordance with procedures established in the USCIS Security Handbook Chapter 8.
4. For policies regarding classified records, see RPM Vol 3, Part C, Chapter 13.
5. There are three levels of classified records:
   a. Top Secret - NSI that may cause exceptionally grave damage to national security if compromised
   b. Secret - NSI that may cause serious damage to national security if compromised
   c. Confidential - NSI that may cause damage to national security if compromised.
6. The overall classification level of a document or record will reflect the highest level of classified NSI contained within the document or record and shall be marked prominently at the top and bottom of the face of the document. For example, a classified document containing Confidential and Secret portions shall be prominently marked "Secret" because that is the highest level of classified NSI contained in the document.
7. Immigration records must indicate the overall classification level conspicuously on the front of the file jacket in addition to a cover sheet attached to the front of the file jacket bearing the appropriate classification level.
8. Top Secret information is subject to access and handling restrictions that do not apply to Secret and Confidential information. All programs storing Top Secret information must appoint a Top Secret Control Officer (TSCO) to manage all Top Secret holdings. Personnel may only access Top Secret materials through the TSCO. For specific instructions regarding Top Secret control procedures refer to the USCIS Security Handbook Chapter 8, Part E.
9. For policies regarding classified records, see RPM Vol 3, Part C, Chapter 13.

Chapter 5 - Catalogue of Immigration Records

1. The Central Index System 2 (CIS2) is a centralized database containing summary data about the existence and status of most aliens known to USCIS, the location of their A-files, and the location of other information pertaining to an alien in other mission-oriented databases.
2. Most, but not all, assigned A# are in CIS2. Some A# predate CIS2.
3. RAILS is the location and tracking system for immigration records.
4. A- and C-files with identical numbers/suffixes DO NOT relate to the same subject, the way A-, T-, Sub-, and W- files relate. The Retired Citizenship (C-number) files listed in RAILS relate to those individuals naturalized prior to April 1, 1956. For example, RAILS may display the following information for A07 354 238:
   a. A07 354 238 Located at NYC > Alien Registration (A-number)

b. C07 354 238 Located at COW > Naturalization Case file (C-number)

5. For detailed guidance on CIS2, refer to the CIS2 User Guide.
6. For detailed guidance on RAILS, refer to the RAILS Quick Reference Guide.

Part B - Creating Immigration Records

Chapter 1 - Empty A-file Jacket Distribution

1. An empty A-file jacket is a preprinted folder. Each empty A-file jacket represents a valid Alien Registration Number. All personnel handling empty jackets must protect each empty A-file jacket from unauthorized access and misuse.
2. Regional Offices under HQ FOD will control distribution of empty A-file jackets to the following offices within their respective regions:
   a. Local USCIS offices;
   b. CBP offices; and
   c. ICE offices that are not FCOs.
3. NBC, also under HQ FOD, will control distribution of empty A-file jackets for its own use.
4. SCOPS will control distribution of empty A-file Jackets for the Service Centers.
5. RAIO will control distribution of empty A-file jackets for the offices within its jurisdiction.
6. NRC under IRIS will control distribution of empty A-file jackets for its own use.
7. AAO will control distribution of empty A-file jackets for its own use.
8. ICE Headquarters Records will control distribution of empty A-file jackets for all ICE FCOs.
9. Upon request from an office authorized to control distribution, WFC will ship empty A-file jackets directly to the requisite FCO upon an approved request.
10. In RAILS, empty A-file jackets can only be shipped in batches of 250, 500, 750, or 1000 per transaction.
11. Offices authorized to control distribution are responsible for ensuring that they regularly track A-file jackets and audit the jackets on a semiannual basis.

Chapter 2 - Responsibilities of Empty A-file Jacket Manager (EJM) and Empty A-file Jacket Coordinator (EJC)

1. The Empty A-file Jacket Manager (EJM) provides empty A-file jackets to other local components within its jurisdiction. Exercising this authority does not absolve the EJM from oversight responsibility for the empty A-file jackets after distribution.

2. The EJM cannot issue empty A-file jackets to local law enforcement officers acting on behalf of ICE. Neither the FCO nor the EJM has the authority or discretion to issue empty A-file jackets to components outside USCIS, ICE, or CBP.
3. The EJM must be a Federal employee.
4. The EJM is responsible for
   a. Accounting for the empty A-file jackets received at the local FCO. This responsibility continues after the EJM has provided them to an external component;
   b. Retaining written documentation of the name and contact information of the designated EJC who receives the empty A-file jackets;
   c. Conducting audits and sending results to the Business Operations and Integration Branch (BOIB); and
   d. Assigning an alternate if absent from the office.
5. Empty A-file Jacket Records Coordinators (EJC) are responsible for
   a. Accounting for the empty A-file jackets issued by the EJM;
   b. Monitoring the empty A-file jacket inventory;
   c. Requesting additional empty A-file jackets from the EJM; and
   d. Assigning an alternate EJC.

Chapter 3 - Requesting Empty A-file Jackets

1. The EJM must not request more than a one-year supply of empty A-file jackets or more than the FCO can store securely.
2. Orders must be placed via the Document Services Management System (DSMS)
   a. Exception: ICE does not have access to DSMS and should send requests to HQPCB-EM@uscis.dhs.gov.
   b. District and Field Office requests must be approved by their Regional Records Office.
   c. Service Centers, International Offices, Asylum Offices, the NRC, the AAO, and ICE FCOs must receive approval from their established Records POCs.
3. The WFC ships empty A-file jackets within 14 business days of receiving the order.
4. Empty A-file jackets must be stored in a GSA approved container or secure area that is locked at all times with authorized access to limited employees.
   a. When a GSA approved container is used, combinations must be protected and changed when an authorized employee departs, there is evidence of theft, or inappropriate access.
   b. When a secure area is used, combinations or keys must be strictly controlled to ensure limited access.
5. Upon receipt of a shipment of empty A-file jackets, you must:
   a. Ensure that the assigned numbers (located on the outside of each box) for the empty A-file jackets match the information on the DSMS manifest outlining the contents of the boxes.

b. Acknowledge receipt of the shipment using Form G-504, Report of Property Shipped-Received, within seven working days if you do not have access to DSMS.
c. Conduct a quality check within seven working days. Damaged boxes or boxes with broken seals must audit every record in that box within 48 hours of receipt.
d. Enter receipt of the new shipment into RAILS ("Receive" transaction) within seven working days.
    i. Ensure the Empty A-file Jacket Block is checked to properly transfer in and account for the shipment as Empty A-file jackets;
    ii. Transfer files in from the FCO "COW;"
    iii. Enter the A-number(s) issued;
    iv. Enter the name of the Records personnel who issued the jacket(s);
    v. Enter the RPC to whom the empty A-file jacket is assigned; and
    vi. Enter the operational unit that received the jacket(s).
e. Conduct a random quality control sampling of ten percent of the newly received empty A-file jackets.
    i. Ensure there are no discrepancies such as duplicate numbers, mismatched numbers, gaps in sequential numbering, missing barcode labels, barcodes that scan a different number, or other printing errors in the shipment.
    ii. Verify that the A-number printed on the front of the folder matches the A-number printed on the barcode label.
    iii. Record any discrepancy immediately.
f. Consult the Records POC to take appropriate steps to resolve any discrepancies.
g. If there is a discrepancy that cannot be resolved locally, send a discrepancy report to BOIB at HQPCB-EM@uscis.dhs.gov with "Empty Jacket Discrepancy" in the subject line. The discrepancy report must include: the FCO, name of the EJM, A-number range on the outside of the box, A-numbers for the files affected, and a description of the problem.

6. RAILS retains file history for up to 10 years. If a written log is maintained, it must be kept for two years after your location no longer keeps empty A-file jackets.

7. FCOs distributing empty A-file jackets to ICE or CBP offices within their jurisdictions must ensure that file jackets are properly tracked in RAILS and that once A-files are created, these files no longer remain in empty A-file jacket status.

Chapter 4 - Managing Empty A-file Jackets

1. The FCO can issue empty A-file jackets in blocks to operational areas upon request. The EJM may establish procedures for making requests.
    a. Form G-504, Report of Property Shipped-Received, must be completed when shipping/issuing empty A-file jackets to an operational area.
    b. In RAILS, use the "Send" transaction, checking the "Empty A-file Jacket" box to transfer the empty A-file jacket(s) to the new location.

c. The requesting operating unit's EJC must receive the jackets in the proper RAILS code as "Empty."

2. Issuing empty A-file jackets to external FCOs
   a. An FCO may issue empty A-file jackets to another FCO in RAILS with proper approval from the directorate chain of command.
   b. Before the transfer is initiated, a copy of Form G-504 must be emailed by the sending office to:
      i. The appropriate directorate chain of command;
      ii. The receiving office; and
      iii. BOIB at HQPCB-EM@uscis.dhs.gov. "G-504" must be in the subject line of the email.
   c. In RAILS, use the "Send" transaction, and check the "Empty A-file Jacket" box to transfer the empty A-file jacket(s) to the new location.

3. Electronic creation of an A-file: Some offices need to create a physical file, but cannot send the file to the Records Unit in the FCO for electronic creation. This is often the case in Border Patrol or Detention and Removal offices where the physical file must stay with the alien in custody. These offices must submit the source document used to trigger the electronic creation of the A-file. See RPM Vol 3, Part B for additional information.

Chapter 5 - Creating A-files

1. A-files are created when an application or petition for long-term or permanent benefit is received or in relation to pending enforcement actions.

2. Only one A-file per individual must exist. Before creating an A-file, you must ensure that the individual does not already have an A-file and ensure that the documents are eligible to trigger an A-file creation. If more than one A-file per individual exists, see RPM Vol 3, Part C, Chapter 6.
   a. If you have documents with one of these older A-numbers (12 million series or between 30,000,000 and 34,999,999) but cannot find the record in CIS2, initiate a manual search request through the ORM Request website.
   b. If a person has an A-number in the one hundred million (100,000,000 – 199,999,999) range issued for Employment Authorization Documents (EAD), these A-numbers are electronic only. No record folder for these numbers will exist; do not create physical folders for these numbers or add them to RAILS.
   c. If a DOS A-number
   d. If there is an existing record(s) in CIS2, you will need to review the record(s) to determine if it is a match before continuing with the A-file creation process.
      i. Pull the record if it is in your FCO;
      ii. If the record is at the NRC, you can contact the Information Liaison Unit to help you determine if the record is a match; or

iii. If the record is in another FCO or the FRC, request the record. Hold on to the material and create a T-file. Verify the T-file relates before connecting the material.
iv. If there is an existing related A-file, request the record. Interfile the material upon receipt.
v. If you do not find a match, continue with the A-file creation process.

3. If a new physical record already has an existing electronic record, update CIS2 with all pertinent information using Data Maintenance (MPER) Screen 9411.

4. The following systems interface with CIS2 to create A-files:
   a. DSI, a Department of State system;
   b. Employment Authorization Documentation System (EADS), a subsystem of the Computer Linked Applications Information Management System (CLAIMS);
   c. Visa Packets through CLAIMS;
   d. Refugee, Asylum, and Parole System (RAPS); and
   e. USCIS Electronic Immigration System (ELIS).

5. The following documents trigger the creation of an A-file:
   a. Form I-130, Petition for Alien Relative;
   b. Form I-485, Application to Register Permanent Residence or Adjust Status;
   c. Form I-589, Application for Asylum and for Withholding of Removal;
   d. Form I-821, Application for Temporary Protected Status;
   e. Form N-600, Application for Certificate of Citizenship; and
   f. Form I-213, Record of Deportable/Inadmissible Alien, that has been entered into the Enforcement Integrated Database (EID).

   Note: this list is not exhaustive.

6. Only source documents originating within DHS can be used to create an A-file. Documents originating outside of DHS, including those issued by other federal government agencies, state and local criminal records, and personal original documents submitted by applicants, are insufficient by themselves to trigger the creation of an A-file. USCIS does not have the authority to verify or validate documents originating outside of DHS.

7. Only Records and designated records personnel can physically create and perform the electronic creation of a physical A-file(s).
   a. Records Unit Supervisors are responsible for ensuring that all records are created physically (if applicable) electronically in CIS2.
   b. Offices must work the RAILS/CIS2 interface reports. These reports show the records in RAILS, but not in CIS2. Obtain the A-file and create it electronically in CIS2.

8. A-files must be physically and electronically created, have the creation verified, and the status updated in RAILS within five working days from receipt of the documents or data that give rise to their creation. The five-day clock starts when:
   a. The application/petition is receipted into CLAIMS3/CLAIMS4 if applicable; or

b. The A-file creation unit receives the trigger document.

9. Each office must have a means of accounting for A-file creations that can provide:
   a. The date an A-file request was received; and
   b. The date of creation for the corresponding A-file.

10. To create a physical A-file, you must:
   a. Create a new folder by obtaining an empty A-file jacket from the EJC;
   b. Enter the electronic data into CIS2;
   c. Verify the creation in CIS2 (within 48 hours after electronic creation);
   d. Enter the location into the tracking system;
   e. File the documents in ROP order
      i. Use prong fasteners to attach documents to the file jacket.
      ii. Small documents or pictures must be taped to a regular 8.5" x 11" size white piece of paper.
      iii. Staples must not be used to attach anything in or to the file.
   f. Eliminate the possibility of DOS issuing duplicate A-numbers by conducting appropriate system searches (See RPM, Volume 3, Part D, Chapter 8, Searching for records) to determine if beneficiaries/applicants an A-numbers exists.
      i. If an A-number exists, you must annotate the pre-existing A-number on the top blank area of the petition/application.
      ii. SCOPS will print and supply barcodes of the A-number or FOD will clearly print the A-number in red ink if a barcode is not feasible.
      iii. If multiple A-numbers exist, annotate only the primary A-number (See RPM, Volume 3, Part D, Chapter 8, Searching for records).
      iv. If no A-number exists, annotate "No A-file number assigned" in red ink on the top blank area of the petition/application.
      v. Address non-compliance issues when the DOS confirms that no notation was found on petitions/applications, by contacting BOIB at HQPCB-EM@uscis.dhs.gov.
   g. After creating a physical A-file, create an entry in the creation log. If the empty file jacket is not yet in CIS2, email a copy of the log to the local Records Unit.

11. To create an electronic A-file, you must enter the data into CIS2. See CIS2 User Guide for additional guidance on New File Add procedures.
   a. There must be an entry in the first and last name fields. Enter the middle name field if available.
   b. If an individual only has one name, enter the name in the Last Name field. In the First Name field, enter "No Name Given". Put spaces between the words.
   c. Names must be alpha characters. Do not use numbers.
   d. Names cannot include punctuation. The system will accept the entry, but it removes punctuation or alters the search without notification to the user.
      i. Use a space instead of a hyphen (-)
      ii. Use "Jr" or "Sr" for Junior or Senior, no period

iii. Use Roman Numerals (for example, "III" or "IV") for numerical suffixes. For example, "Joe Johnson, the 3rd" would be written "Joe Johnson III"
iv. Spell out a number if used for a name. For example, if the name is 8, enter "Eight" in the last name field and "No Name Given" in the first name field
v. Spell out a symbol if used for a name. For example, if the name is ★, enter "Star" in the last name field and "No Name Given" in the first name field.

e. Do not add spaces at the end of a name field as CIS2 recognizes the space as an invisible character.
f. If the person has more than one alias, after you validate the CIS2 entry, enter the additional aliases using Alias (AKA) Add Screen 9303.

12. Updating physical A-file status in RAILS
a. File status must be updated from an empty jacket status to an active status.
b. In the hybrid records environment, an electronic system such as ELIS, EDMS, or STACKS may serve as the official A-file immigration record. However, applicants frequently submit additional applications and evidence which are not currently supported by electronic processing or maintenance, and; therefore, must be retained in a physical format. In these cases, physical A-files must be created using the A-file number assigned to the applicant (identity) in the electronic system to store documents not supported by ELIS, EDMS, or STACKS.
Note: Conducting a search in RAILS will indicate all related official physical and electronic A-files. This serves as sufficient notification that there is a hybrid record consisting of both paper and electronic A-file material.
c. This process will create a hybrid A-file, partially in the electronic system and partially in paper format; together all parts will constitute the entire official immigration record that is unique to an individual identity.
d. Hybrid files can also be created:
vi. ELIS record exists and EDMS has corresponding A-file: When additional A-file material is received and cannot be uploaded into ELIS, a T-file must be created. When the office no longer has a need for the file, the T-file must be sent to the NRC for storage and scanning into EDMS. See RPM Vol 4, Part B, Chapter 3 for more information.
vii. ELIS record exists and EDMS has corresponding Receipt file: When additional A-file material is received and cannot be uploaded into ELIS, a physical A-file must be created using the A-number assigned to the applicant in ELIS.
e. Do not incorporate official USCIS electronic A-file material (contained in ELIS or STACKS) into the physical A-files. Do not print ELIS, EDMS, or STACKS records and create or place the material into physical A-files. All supporting A-file material must be uploaded into ELIS where supported and may only be placed into a physical A-file when an official ELIS record does not exist or material cannot be uploaded to the digitized or electronic record.

f. A-numbers between 80,000,000 and 86,899,999 will no longer be designated as "electronic only". This range of A-file numbers can be added to RAILS using the "Add File" transaction and combined with physical file(s) as needed.
   i. When a triggering document is received for an individual with an existing 80 million number who does not have a second A-number related to a physical file or electronic record (ELIS or EDMS), the 80 million number is the primary A-number. The existing number must be added to RAILS and a physical file created. A new number must not be issued/assigned.
   ii. When an existing physical 80 million number file is found that was not previously in RAILS, it must be added to the system. If the individual also has a second A-number related to a physical file, the two files must be consolidated. See RPM Vol 3, Part C, Chapter 6.
   iii. If an individual has a physical record for both an 80 million number file and an additional number, the two records must be consolidated. See RPM Vol 3, Part C, Chapter 6 to determine which number to use as the primary.

13. After the file has been created and updated in RAILS, it must be verified.
   a. An A-file cannot be created and verified by the same person.
   b. To verify the electronic record:
      i. Use the Verification (VERF) 9302 Screen to verify the new add; and
      ii. Check CIS2 9101 screen to verify the electronic creation.
   c. To verify the physical record:
      i. Verify the record history stamp appears on the inside left cover of the A-file jacket. If there is no history stamp inside the left cover, write “Verified”, your initials, and the date;
      ii. Verify the person who created the record in CIS2 has annotated the physical record with their initials, the FCO, and the date;
      iii. Annotate your initials, the FCO, and the date of verification;
      iv. If the file jacket is not available, as an interim action, annotate the creation document.

Chapter 6 - Creating Other Immigration Records

1. Creating a T-file
   a. Create the physical T-file
      i. Use colored file folders to distinguish T-files from A-files
      ii. For odd-numbered files, use a folder with a left tab. For even-numbered files use a folder with a right tab.
      iii. Place barcode labels on the front and back tabs of the folder, using the same number as the A-file preceded with a “T” instead of an “A.” For example, the label for a T-file for A-file A12 345 678 will be T12 345 678.

iv. Attach the material in ROP order using an Acco-type fastener. If you are consolidating the Receipt file into the T-file, first create the T-file in the system, and then follow the processes for electronic consolidation.

b. Create the electronic T-file by adding the T-file number to RAILS. See RAILS Quick Reference Guide: Adding Files for additional information.

c. There are three situations in which you create a T-file:
   i. A search shows that your office is the FCO for an A-file and after a complete search, the file cannot be found. You also need to ensure there is not another T-file for the same A-file.
   ii. You requested the A-file from another office and, while waiting for it to arrive, you need a temporary place to house an application, petition, or an enforcement action.
   iii. If your local procedures specify that an adjudicative decision can be made on a T-file when the A-file is not available. For example, when a T-file is created for adjudication of Naturalization cases (follow the NQP request process before creating a T-file).

d. Do not create a T-file if there is no corresponding A-file or Sub-file.

e. It is best to have only one T-File; otherwise the documentation on the person gets fragmented. There is a danger of people making decisions without full information.

f. Only Records personnel may create a T-file. This applies to both the physical and electronic creation tasks.

g. Do a search before creating T-file.
   i. Check RAILS to see if another A-file, Sub-file, or T-file exists in your office.
      - If no other T-file, Sub-file, or A-file exists in your local system, you will see the message No Master Record or FRC Record Found.
      - If there is an A-file, Sub-file, or T-file in your FCO, do not create a T-file. Request the file.
   ii. Check CIS2 9504 screen for an A-file.
      - The CIS2 FTD screen accessed by selecting PF11 from the 9504 screen will no longer be updated with file location and status information. The CIS2 FTD data froze on the date CIS2 deployed, but will be available to CIS2 users to query for historical purposes.
      - If you find it, request the A-file. See RPM Vol 3, Part D, Chapter 1. You can make a T-file in the interim.
      - If there is no A-file, create one if the document triggers an A-file creation. See RPM Vol 3, Part B.

h. If you already have a T-file and need to merge it with the A-file, follow the directions in File Consolidations, Combinations, and Deconsolidation.

2. Creating a Substitute file (Sub-file)
   a. Authorization to create a Sub-file
      i. A District Director (FOD), Service Center Director (SCOPS) or USCIS Program equivalent must authorize the creation of a Sub-file.

ii. The ability to authorize Sub File creation can be delegated locally to the District Records Manager (FOD), the Associate Center Director supervising records management (SCOPS), or USCIS program equivalent supervisor over records management. The delegation shall occur in writing and the office must retain this delegation letter locally.

iii. A memo requesting creation must be placed in the Sub-file. The memo must include:

- A-number;
- If the file was destroyed, the date and cause of destruction;
- If the file is lost, a written account confirming that a special search was conducted and that RAILS has been updated using the appropriate transaction;
- Signature of Field Office Director or USCIS program equivalent requesting the creation of the Sub File; and
- Signature of the person authorizing the creation of the sub file.

b. Create the physical Sub-file

i. Blank A-file jackets (like those used to replace damaged A-file jackets) are ordered from WFC via the Document Services Management System (DSMS). Left and Right tab folders must be ordered separately in multiples of 250. Left tab folders are Position 1, item M-672B1; and Right tab folders are Position 3, item M-672B3.

ii. If using a file jacket that was not received from WFC for the replacement, use a brown heavy gauge folder similar to a pre-printed A-file jacket. Use a left tab folder for odd numbered files and a right tab folder for even numbered files. The folder must be stamped with the following in 1/4 inch letters:

PROPERTY OF THE U.S. GOVERNMENT
IF FOUND RETURN TO:
DEPARTMENT OF HOMELAND SECURITY
U.S. CITIZENSHIP AND IMMIGRATION SERVICES
NATIONAL RECORDS CENTER
150 SPACE CENTER LOOP
LEE'S SUMMIT, MO 64064

iii. Place barcode labels on the front and back tabs of the folder, using the same number as the A-file preceded with an "A" instead of an "A." For example, the label for a Sub-file for A-file A12 345 678 will be S12 345 678.

iv. Mark the front tab of the folder with a stamp that reads "SUBS."

v. Mark the jacket face with a stamp that reads:

ORGINAL FILE CANNOT BE LOCATED
SUBSTITUTE FILE CREATED
DATE _____

SIGNATURE _____

vi. Add material in the new sub-file in ROP order using an Acco-type fastener. Contact the appropriate program office to obtain previously submitted documentation and print all pertinent documents that are unable to be obtained.
vii. Place the memo approving the Sub-file creation on the right side of the file Check applicable databases/systems and

c. Create the electronic Sub-file by adding file to RAILS using the "Add File" transaction.

3. Creating a Receipt file
   a. A Receipt file number is assigned by CLAIMS when the application or petition is keyed into the system.
   b. Create the physical file by placing barcode labels on the front and back tabs of a folder, using the CLAIMS-assigned receipt number.
   c. Create the electronic file in RAILS using transaction "Add File."
   d. The Receipt file numbers consist of the following:
      i. Three letter prefix for the Centers;
         - **LIN** Nebraska Service Center
         - **EAC** Vermont Service Center
         - **WAC** California Service Center
         - **SRC** Texas Service Center
         - **MSC** National Benefits Center
         - **YSC** Potomac Service Center
      ii. Two digits signifying the year;
      iii. Three digits signifying the Julian date; and
      iv. Five digits indicating the sequence.
   e. An example of a receipt number is LIN-98-123-58970.

Chapter 7 - Barcodes

1. Barcode basics
   a. Barcoding is an optical Morse code. It uses black bars and white spaces of varying widths and sizes. A scanner passes over the code and, measuring the reflected light, interprets the code into numbers and letters that pass on to a computer.
   b. Barcodes also need to have a quiet zone or blank area before and after the barcode. This is essential so the barcode reading device can identify where the barcode stops and starts. Barcodes printed too close to the edge of a label may be unreadable.
   c. USCIS, Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) use the most common type of barcode, known as Code 39 also referred to as 3 of 9.
   d. These components use three types of barcode information:
      i. Number labels for file folders;
      ii. Labels for responsible party codes; and

iii. Barcode menus that allow the user to wand in a transaction code rather than key the transaction code into RAILS.

e. Only one (surviving) A-file jacket number barcode can be placed on the outside of the folder. Incorrect uses of barcodes are seen, for example, where offices place the receipt file barcode on the outside of the A-file jacket, which if scanned during an audit, causes a variety of tracking issues and potential errors.

2. Using hand-held or wand barcode scanners
   a. If you are using a pencil wand, move the wand across the entire barcode. If the wand does not read the barcode, try moving the wand across the barcode slower. Most scanners give an audible beep (one beep) when it reads the code successfully. Try not to rub the wand against the label. If you have to rub the wand against the label, do so lightly.
   b. If you are using a hand-held wand, point the wand at the barcode and then pull the trigger making sure the beam crosses each black bar of the barcode. If the hand held wand does not read the barcode, try adjusting the angle.

3. Using portable barcode scanners
   a. Before using portable barcode scanners:
      i. Fully charge the scanner;
      ii. Erase previous information;
      iii. Program the scanner for the appropriate function; and
      iv. Review the date and time. Follow the prompts to insert the correct date and time, if needed.
   b. Upload scanner data before the memory is completely full or the battery runs down. The local Records Office or local RAILS Administrator can assist with uploading the data.
   c. For more information on the new Dolphins, consult the manuals Dolphin 7850 or Dolphin 7200 (these are large PDF files and may take time to download).

Chapter 8 - Record of Proceedings (ROP)

1. A Record of Proceeding (ROP) is the official history of any hearing, examination, and/or legal proceeding in order to show cause or adjudicative action in conjunction with any immigration action taken by DHS.

2. ROP materials constitute the comprehensive record of any application, petition, or hearing before DHS or DOJ, that is EOIR.

3. ROP materials must be kept intact and are critical for many critical functions, such as efficiently and accurately adjudicating benefit applications; creating CTCs; responding to FOIA requests; supporting law enforcement actions, investigations, and litigation; and dispositioning records in accordance with NARA policies and relevant retention schedules.

4. Program Offices are responsible for determining and assembling form-specific ROPs and will place it on the left side of a paper A-file.

5. You may not disassemble or add materials to an ROP without specific instructions from the Program Office.
6. Any partial or fully electronically filed elements of the ROP must be housed in one of three NARA compliant repositories: EDMS, ELIS, or STACKS. No other system may be used for this purpose without approval from IRIS.
7. The ROP of a particular application or petition may not be interspersed among multiple electronic repositories; it must be contained within a single such repository.
8. Records units are responsible for:
   a. Assembling newly received applications and petitions in the ROP order specified by the Program Office;
   b. Ensuring a document relates to the record before adding it the folder;
   c. Maintaining the ROP, not rearranging the order of documents;
   d. Putting documents on the correct side of the record folder; and
   e. Adding interfiling.
9. Record assembly
   a. If the ROP does not designate left-side or right-side of the folder, then place all specified documentation on the left side of the folder and un-specified documentation on the right side of the folder in reverse chronological order. Note: the location of the document (right side versus left side) does not impact whether or not the information can be released to the individual or another agency. These are Privacy Act/FOIA determinations.
   b. If the Program Office has not designated an ROP, assemble the following documents (if applicable) on the left side from top-to-bottom:
      i. G28, Notice of Appearance as Attorney or Accredited Representative;
      ii. Pending Request for Evidence (RFE) notices and Intent to Deny notices;
      iii. Initiating Document (the application, petition, charging document, or other form/document that initiated the action the ROP pertains to); and
      iv. Supporting documents in reverse chronological order (most recent first).
   c. Visas and their supporting documents are not ROPs and should be placed on the right side of a file, not the left.
   d. M-175, Cover Sheet-Record of Proceeding, must be placed on the top of each ROP.
      i. If there is an N-400, it is always on the top of the left side of the file.
      ii. If the file jacket contains classified material, follow the procedures for filing and marking classified material.
   e. If the folder contains any classified material, the entire folder must be treated as a classified record. See RPM Vol 3, Part C, Chapter 13 for additional guidance.
   f. If the information is restricted but not classified, put it in a brown envelope marked Restricted Material Pertinent to (Type of application/petition and the date of the application/petition). The envelope will be on the right hand side of the record.

g. Maintain Legalization/Special Agricultural Worker (SAW) material in reverse chronological order underneath all regular documents on both sides of the file jacket.
    i. The Immigration Reform and Control Act of 1986 gave certain individuals the right to apply for legal status. The legalization records are A-files created when people applied for legalization. Most of these files have a number between A-90, 000,000 and A93,999,999.
    ii. Use a red Form M-330, A-file Cover Sheet, to separate the legalization material from the post-legalization material.
    iii. Use the pink M-175, Cover Sheet-Record of Processing above the red cover sheet for the post legalization ROP.

h. Do not confuse a ROP with a batch of interfiling.
    i. An ROP is generally fastened with a prong fastener and typically pertains to one person and a specific action.
    ii. Interfiling contains multiple documents, often fastened with a rubber band, clip, or staple.

Part C - Managing and Maintaining Immigration Records

Chapter 1 - Storing Records

1. Department offices use one of two systems to arrange Records:
    a. Responsible Party Filing System (RPFS) – the Department standard used for filing records, based on RAILS, and the USCIS required method.
    b. Terminal Digit Order (TDO) system – only authorized to use in conjunction with RPFS.
2. The Section Code and Responsible Party Code (RPC) identifies each possible record location within the RPFS. Anyone requesting or working with records must have a Section Code and an RPC.
    a. ICE must use the following Section Codes:
        i. DD for Enforcement and Removal Operations (ERO);
        ii. IV for Homeland Security Investigations (HSI); and
        iii. LI for the Office of Principal Legal Advisor (OPLA).
    b. The two ICE units unique to COWREC may also use the following Section Codes:
        i. GC for the Office of General Counsel; and
        ii. PB for the Parole Branch.
3. RAILS keeps track of records housed within the RPC, the section, and the location of that code, so RPCs can also be assigned to
    a. a section of shelf or file room,
    b. an operational unit workstation,
    c. a bucket,
    d. a staging area,
    e. a safe,

f. or another location designated by management.

4. Each office is responsible for maintaining the RPFS. The office assigns new RPCs as needed.

5. The RAILS Data Administrator in the Records Unit maintains the RPCs. For procedures and more information on RAILS, see RAILS Connect site

6. Converting an office to the Responsible Party Filing System (RPFS)
   a. When an office receives the RPFS for the first time: when an office initially receives RAILS, the office is responsible for implementation. The Region will ensure the office receives the necessary training.
   b. When planning the file room, use the RPFS. The following is a brief list of options.
      i. Sort each RPC by TDO;
      ii. Separate odd/even tabs;
      iii. Segregate A- and T-files;
      iv. Segregate Receipt files;
      v. Segregate by application/petition type; or
      vi. Segregate by operational unit.
   c. Installation of the RPFS involves the following steps:
      i. Create a map of the area being converted to the RPFS. This will help with deciding where to put each individual RPC.
      ii. Create all RPCs in RAILS in accordance with the map created.
      iii. Label the end panel of each row of shelving to make it easy to locate records. For example: Row AA001-100, Row AA101-199.
      iv. Install dividers (preferably at one-foot intervals) in the shelving section to delineate each RPC throughout the entire file room.
      v. Ensure all labels are in numerical order.
      vi. Attach the RPFS barcode audit labels (left justified) to shelving units for each RPC throughout the entire file room.
      vii. Relocate the records by shifting them into the RPC. A one-foot section can hold approximately 50 records.
      viii. Audit the records into each RPC using the portable bar-code readers and the non-sequential audit program.

7. File rooms using TDO in conjunction with RPFS
   a. If using TDO, the options include:
      i. Arranging the records on open shelving in TDO; or
      ii. Putting odd-numbered records on one side of the aisle and the even numbered records on the other with tabs facing the aisle.
   b. Mark shelves to indicate the beginning and ending of a TDO section (that is, separating the TDO of records ending in 726 from 727).
   c. As a quality control measure, check the numerical sequence of records on a regular basis and return misfiled records to their proper location.

8. Records centralization, storing records, and the NRC
   a. Records centralization changes how the Department manages records. A large file room with records stored for long periods is no longer the norm. Now most A-files will be at the National Records Center (NRC). For the local Files Control Office (FCO), emphasis is on managing record circulation with the NRC and maintaining accountability for local records.
   b. Circulation management requires that the local FCO keep only those A-files where an action or decision is pending and those staged for shipment to the NRC or FRC.
      i. Circulation management is an extremely important function of the local records program. Records personnel must constantly monitor the status of records in the local office in order to identify records ready for return to the NRC or retirement to the FRC. Ensuring a steady flow of records back to the NRC once the operating units finish using them, is key to the long-term success of centralization.
      ii. To minimize the number of records requested – and subsequently returned, the NRC provides Information Management Liaison Services as an alternative to requesting a physical record folder. Liaisons are available to Service personnel 24 hours a day, 7 days a week.
   c. When a file is no longer needed for an action it goes to a staging area. Staging areas are set-up to organize files before shipment to the NRC or FRC. Put the records eligible for retirement in the FRC staging area. Stage the other records in the NRC staging area
   d. Record accountability means closely monitoring how long operating units keep their records and how well they track them. Auditing plays an important role in maintaining record accountability.

Chapter 2 - Closed Records

1. Only A-files that are closed can be shipped to the NRC.
   a. To ensure the case is closed, you must check the applicable system (for example, CLAIMS or WRAPS) and review the physical record for the most recent application or petition for an approval stamp, denial letter, or other applicable method of identifying closure of the pending application.
   b. If an associated active case/open petition for benefits is found, the record must be returned to the appropriate operating unit for processing unless no action on the matter is anticipated for at least six months.
   c. Records must not be staged for shipment to the NRC for more than 90 days.
   d. NOTE: Closure of Form I-590, Registration for Classification as a Refugee, is indicated by one of the following methods:
      i. Cases approved digitally via WRAPS will be accompanied by a Digital Approval Event Report. This report signifies approval in lieu of traditional stamps.
      ii. The traditional ink approval or denial stamp in the upper or lower action block of the paper form will continue to be accepted.
   e. Check with the last operational unit that had the record if you have any questions.

2. Currently, the staging time for inactive records varies from office to office. The recommended period to stage and prepare records for shipment to the NRC is 30 days.
   a. In deciding on a staging period consider the amount of space on hand and the cost for shipping the record.
   b. Assign the records to the RPC for the staging area using RAILS.
   c. Once records have been on the shelf for the staging period, they are eligible for shipping to the NRC.
   d. The Records Office may choose to run the Aged File Holdings by Section or Responsible Party Report on the Reports Menu in RAILS Records Management Dashboard. This report lists files under RPCs for the period (0-3 months to over 3 years) you designate. This helps identify records that have not been moved and could be shipped to the NRC or retired to the FRC.
   e. Pull the identified records and prepare them for shipping to the NRC.
   f. See RPM Vol 3, Part G, Chapter 2 for information on how to identify records eligible for retirement and the process to follow for retiring them.
   g. Keep these records in a separate staging area.
3. Changes in local procedures after mass record moves
   a. Moving the bulk of records to the NRC means adjusting local procedure for record requests, record returns, and record retirements, among others.
   b. The Records Supervisor has the responsibility for initiating the changes in local records procedures, documenting them, and making local users aware of them.
4. Only receipt files that are closed can be shipped to the HBG.
   a. To ensure the case is closed, you must check the applicable system and review the physical record for the latest application or petition for an approval stamp, denial letter, or other applicable method of identifying closure of the pending application.
   b. If the case is not closed (either in the case management system or the physical record) or an associated active case/open petition for benefits is found, the record must be returned to the appropriate operating unit for processing.
   c. Approved receipt files must be held for 15 days before shipping to HBG
   d. Denied receipt files must be held for 90 days before shipping to HBG
5. A-file Refiling
   a. Refiling
      i. Refiling procedures vary depending upon whether the office has: RPFS filing or TDO filing.
      ii. Refiling, in most cases, means putting the file in the staging area for the NRC or FRC.
      iii. Many offices will move records from one location to another as part of the workflow involved in processing an application or benefit. These will be internal moves. Follow local procedures.
      iv. Refile all A-files and Receipt files daily.

v. Inspect Teams review refiling backlogs at each site during an inspection. The team will verify the office that:
   - Records are in the location reflected in RAILS; and
   - Refiling is done daily.

b. Preparing records for refiling
   i. Most file rooms assign returned records to a temporary RPC when staging them for refiling.
   ii. Remember records returned from internal operating units or transferred in from outside offices are received into RAILS ("Receive" function).
   iii. With RAILS, if you Transfer In a record that is already in RAILS, RAILS thinks it is a duplicate record. The system will ask if you meant to add a duplicate or if you made an error. If the file is a duplicate, follow your local procedures for handling duplicate records.
   iv. Check to see if any of the records need maintenance such as:
      - A new barcode label;
      - An additional volume (for folders that are too full);
      - A new jacket; or
      - Consolidations or mergers
   v. Check for any current routing slips asking to have the file sent to another person, operational unit, or another specific location. If there are any, use the appropriate function in RAILS to "Send" the record.
   vi. Sort the records into odd and even numbered groups. Separate T-files and any other records kept in specific responsible parties.

6. Using a portable barcode scanner
   a. In the record room, find available shelf space in a Responsible Party section that can accommodate the files you need to shelve. Usually odd-numbered folders are on the left and evens are on the right. Your record room may have specific responsible parties for certain types of records.
   b. After identifying an appropriate space, log onto a portable bar-code scanner (PBCS).
   c. Wand the barcode label on the Responsible Party section shelf.
   d. Wand the record barcode labels. This connects the records to this shelf location.
   e. After scanning the record, and before scanning the next responsible party, press the END key on your portable barcode scanner. If you do not, then the barcode reader will read the next location code as a file folder.
   f. After finishing, log off the reader.
   g. Follow the procedures for uploading the data.

7. Uploading portable barcode scanner data into RAILS
   a. After you finish refiling, upload the portable barcode scanner data into RAILS using the Batch Audit Function (RAILS "Batch Receive" transaction).
   b. For details, see the RAILS training video.

c. The upload process adjusts the location of the record from the generic RPC to the file's current RPC in the record room.
d. After completing the upload, RAILS automatically generates the Audit Verification Report (Report Number 481). Use this report to help record refile counts on the G-22 report for line item 700.6. The numbers for 700.6 are cumulative for the entire month. On a daily basis, follow your local procedures for recording the number of files refiled and the number of hours it took to prepare, refile, and reconcile any errors.
e. RAILS does not produce an audit report. All items requiring additional action are displayed on screen after uploading the audit data. RAILS may indicate there is a duplicate record. In this case, follow the procedures for handling duplicates. Correct all errors on screen prior to completing the transaction.

8. Audit verification report for refiling
NOTE: In RAILS, the below corrective actions are performed as part of the "Batch Receive" transaction.
a. The Audit Verification Report contains all record numbers scanned by the PBCS, the audit date, and the action taken.
b. The report shows the old and the new location of the records. The old location should be the generic RPC for refiling. The new location should be an RPC in the file room.
c. Reconcile the Audit Verification Report.
d. Occasionally the Audit Verification Report indicates the old location as other than the initial generic RPC. This can happen if the portable barcode reader scans the barcode incorrectly or there is a duplicate record. Verify the true location of the file by physically checking the locations. Take the corrective action shown in the chart.

File in Old Location	File in New Location	Remedial Action
Yes	No	Update RAILS with the correct (old) file location or move the file to the new location.
Yes	Yes	Pull both records. Check that the barcodes are correct. If not, correct them. If the records are duplicates, stage them for merger.
No	Yes	No corrective action is needed.

e. On the Audit Verification Report, Record Modified, Section Changed should be the only action taken. If Record Added-Available In Records shows as the action for a record, the record was added to the database. Either it was not transferred in initially or the portable barcode reader scanned the record incorrectly. Physically check the record and location and take the corrective action shown in the chart.

File is in Location	Barcode Label is Correct	Corrective Action
Yes	Yes	The record was not Transferred In, Update CIS2 (File Transfer Maintenance). This is a restricted function. Change The PREVIOUS FCO to the FCO showing in Current FCO. Then change the Current FCO to your FCO. Make sure the FILE LOCATED IND is C. Change the DATE FTC to the date of the audit.
Yes	No	The bad barcode belongs to a real record. CIS2 needs to accurately reflect where that record is. Right now CIS2 thinks your FCO has the record. To find out where the record needs to go, access CIS2 TRKS, which is a restricted function. Find out where the bad barcode originated using the transaction history. Update CIS2 using (File Transfer Maintenance). This is a restricted function. Change The PREVIOUS FCO to the FCO before the bad code originated. Then change the Current FCO to the FCO where the bad bar code originated. Make sure the FILE LOCATED IND is C. Change all the dates using the TRKS information. Correct the barcode. Delete the incorrect file number from RAILS. Then Transfer In the corrected barcode using the correct RPC.
No	N/A	If you physically verify that there is not a record with this number in this location, this probably means the PBCS scanned the file incorrectly. Completely audit the RPC. Auditing will locate the records and update RAILS. If this process "finds" the record, take no added action. If the number was erroneously added, delete it from RAILS.

9. Refiling without a portable barcode scanner
   a. Assign a specific RPC to the records before re-shelving. Use your local procedures for doing this.
   b. Use RAILS "Receive" function to receive in the records to the assigned RPC.
   c. Put the records in the assigned RPC.
10. Refiling with the TDO filing system
   a. Sort the files into TDO.
   b. Remove the G-102, File Routed on Loan, from the charge out file and the front of the folder.
   c. Take the files to the file room and shelf according to the TDO file number.

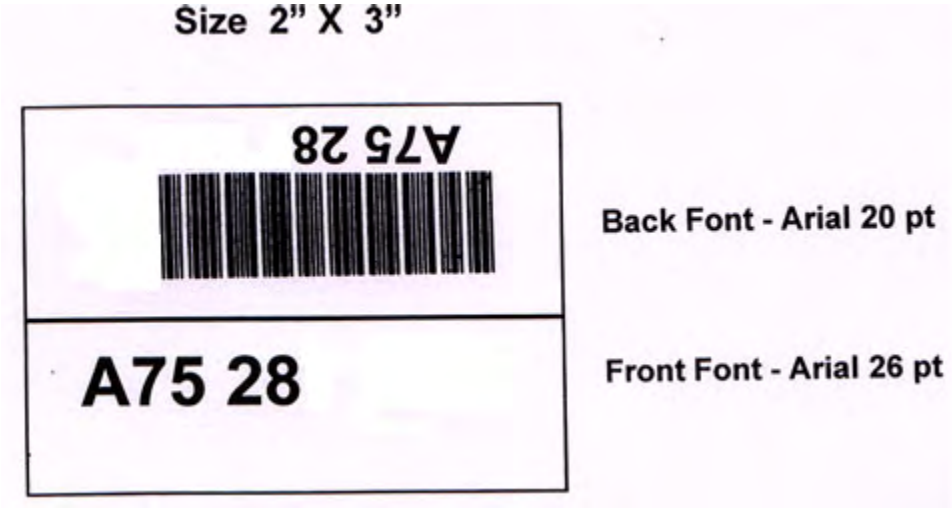
11. PAS reporting
    a. Keep track of the records received for refiling during the month.
    b. Add the number of records re-shelved and the time required to G-22, Workload Record, line 700.2, File Movements.

Chapter 3 - Maintaining Records

1. Only Records Unit personnel may replace worn, damaged, or over-sized (more than 3.5") files.
    a. File jackets must be replaced when the jacket is contaminated, torn, or worn.
    b. Follow the process for over-sized files when the file jacket measures approximately 3 1/2 inches and the integrity of the jacket's stability is compromised.

2. Replacing damaged file jackets
    a. Empty file jackets without pre-printed A-numbers must be used when replacing worn or damaged A-file jackets.
        i. Order blank A-file jackets from Western Forms Center (WFC) by using the Document Services Management System (DSMS). For more information about DSMS, see DSMS website.
        ii. Left and right tab folders must be ordered separately in multiples of 250.
            - Left tab folders are Position 1 and are item M-672B1.
            - Right tab folders are Position 3 and are item M-672B3.
    b. Use a left tab folder for odd numbered files and a right tab folder for even numbered records.

3. Offices must use file jackets received from the WFC. If a situation requires immediate file creation and WFC file jackets are not available, you must use a brown heavy gauge folder similar to a pre-printed A-file jacket.
    a. The folder must be stamped in 1/4 inch letters, Times New Roman font, with the following:
    PROPERTY OF THE U.S. GOVERNMENT
    IF FOUND RETURN TO:
    DEPARTMENT OF HOMELAND SECURITY
    U.S. CITIZENSHIP AND IMMIGRATION SERVICES
    NATIONAL RECORDS CENTER
    150 SPACE CENTER LOOP
    LEE'S SUMMIT, MO 64064
    b. Stamps may be ordered from an FCOs regular office supply company/catalog or any commercial supply company (for example, Staples, Office Depot, et cetera).
    c. The A-number must appear on the front in Arial 26-point font.
    d. The A-number and matching barcode must appear on the back in Arial 20-point font.
    e. Follow local office procedures to create the new barcode



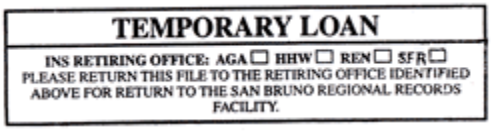
f. Verify that the barcode label number exactly matches the printed A-number on the A-file jacket (front tab).
g. The new file and jacket must mirror the old file and jacket, including any stamps or stickers and all materials in the same order.
h. Arabic Numerals (1, 2, 3, et cetera) must be used to designate each part of a multi-part record.
    i. The part number must be listed on the tab following the A-number. For example, A123456789-1 and A123456789-2.
    ii. RAILS must be updated to indicate all parts.
i. Use an Acco-type fastener. Do not staple material inside the new jacket. Staple or tape small items to a blank sheet of paper before inserting them into the record.
j. The pre-printed file history form on the inside of the file jacket must be completed to show who replaced the file.
    i. You must include the FCO and your initials.
    ii. The NF for New File should be marked out as the file jacket is being replaced and does not apply in this instance.
    iii. If the inside file jacket does not include a file history form (or preprinted stamp), you must create a file history form on a sheet of paper include it in the file.

File History Stamp

NF	FCO	Date	Initials
Verf		Date	Initials
CONS A#	FCO	Date	Initials

k. The old jacket may have stamps or stickers on it. The following are some types of labels that may need replacing and the conditions where it is not necessary to replace the labels:
   i. Form M-125, Under Docket Control at ____ (FCO). This sticker shows that the subject of the record is under deportation docket control. Deportation removes this label when the removal is complete and the record is closed. If deportation has returned this file to the Records Unit, check with Deportation to see if the file is actually still under docket control. If not, do not replace the label.
   ii. Form M-126, Private Bill. This sticker shows a pending Private Bill action. The operating unit removes this label when the action is completed. If the unit returned this file to the Records Unit, check with the operating unit to see if the file of the Private Bill is still pending. If not, do not replace the label.
   iii. Form M-127, Investigations Call UP (C.U.). Investigations put this sticker on the record and pencils in the call up date. If Investigations has returned this record to the Records Unit, check with Investigations to see if the record still has a call update. If not, do not replace the label.

l. If the record is from the Federal Records Center in San Bruno and the operating unit is finished with the record, you must return the record to San Bruno after repairing the jacket. Replace Bond Posted stamps on the outside front of the file jacket (this can be hand written) which appears as follows:
   i. BOND POSTED; and
   ii. DATE.



m. Proper disposal
   iii. To maintain the history contained on the inside front cover of the damaged jacket to the new jacket, attach any and all documentation (bar code, history stamp, et cetera) from the secondary file to the interior of the A-file.
   iv. Properly dispose of the remaining blank portions of the secondary file jacket.

4. Take extra care when handling file folders to protect the barcodes from damage. Stains, staples, or writing on the barcode adversely impacts the ability to scan.
   a. If a barcode becomes damaged, un-scannable, or does not match the number on the record, prepare a new barcode label. Follow local office procedures to create the new barcode label.
   b. Thoroughly inspect new barcodes. The barcode number must match the A-number and the prefix printed on the jacket. Be sure the same number is on both the back and front of the jacket.

5. Handling of over-sized records
   a. Over-sized record: an over-sized file that exceeds approximately 3 ½ inches in thickness. This is a discretionary measurement that is based on not exceeding the Acco-fasteners of a standard A-file jacket. Increasing the volume of file contents should be evaluated to determine whether additional full documents could be added without compromising the integrity of the standard file jacket.
   b. For policy related to the use of locally purchased, oversized jackets, refer to the Interim Policy for Creating Oversize A-file Jackets.

6. When to begin a second record
   a. When the contents of a record (if using standard sized jacket) measures larger than 3 ½ inches and the inclusion of additional documents could compromise the stability of the file jacket, the Records Section should create subsequent record parts.
   b. See RPM Vol 3, Part B, Chapter 3 for guidance on ordering blank jackets.
   c. See RPM Vol 3, Part B, Chapter 4 for guidance on labeling blank jackets.

7. Proper marking of record parts
   a. Use Arabic Numerals (1, 2, 3, et cetera) to designate the parts of the record. Write the Arabic numeral on the tab following the A-number to clearly indicate that there is more than one part to the record.
      i. A new jacket will be used and marked Part 2 of 2.
      ii. The original record will be closed and marked Part 1 of 2.
      iii. Put a Form M-134, File Continuation Sheet, on each side of the record, on top of the material in each continued part. On the File Continuation Sheet show the next part (continued under Part 2, Part 3, et cetera) and the date this part was closed.
   b. In order to help safeguard the Agency's records all subsequent record jackets should be stamped with the following information using ¼ inch letters:
      PROPERTY OF THE U.S. GOVERNMENT
      IF FOUND RETURN TO:
      DEPARTMENT OF HOMELAND SECURITY
      U.S. CITIZENSHIP AND IMMIGRATION SERVICES
      NATIONAL RECORDS CENTER
      150 SPACE CENTER LOOP
      LEE'S SUMMIT, MO 64064

c. Do not use rubber bands to keep record parts together. Some suggestions are to use ½ inch nylon strap with a buckle, twine, or plastic bands to bind together multiple record parts.

Chapter 4 - Duplicate A-numbers

1. Errors may occur in any part of the record or at any point of the file's lifecycle. If an error(s) is discovered, it must be corrected immediately by the office in possession of the file.
   a. Always review the file to determine the accuracy of the data; and
   b. Immediately update appropriate electronic systems (that is, CIS2, CLAIMS, RAILS, et cetera) to reflect the correct data.
2. Resolving duplicate A-numbers
   a. Periodically, personnel may encounter the existence of files with duplicate A-numbers. Duplicate A-number assignments arise due to a variety of causes, including but not limited to the following:
      i. Key-In Entry Errors: Transposed numbers or accidental mis-keys, human error, or errors originating in the source document.
      ii. System Interface Errors: Data is not properly transferred to the intended system during interface.
      iii. Pre-CIS2 files: One of the duplicate file numbers was issued prior to the existence of the Central Index System 2 (CIS2). A file may be categorized as pre-CIS2 if the following apply:
         - File number is 12 million and below;
         - File number is between 30 and 34 million;
         - Individual arrived prior to 1975; or
         - Individual naturalized prior to April 01, 1956.
   b. The Service Center/National Records Center (NRC) Compaction Project: This project entails the National Records Center (NRC) recall of previous retirements performed by other FCOs.
      i. When these records are encountered, a File Control Office (FCO) must request and review all files for resolution.
      ii. If necessary, refer the case to the Adjudications Unit for investigation and assignment of a new A-Number where appropriate.
      iii. If fraud is suspected, an FCO must forward the files to the local Fraud Detection and National Security (FDNS) officer.
3. If duplicate A-file assignments are discovered by the NRC, the record must be sent for resolution to the FCO that performed an action on behalf of one of the customers associated with the duplicate A-number.
4. ICE and CBP offices that discover records with duplicate A-numbers must refer the issue to their local Records office.

5. If duplicate A-file assignments are discovered, the following must occur:
   a. An electronic merge must be performed in RAILS using the Combine transaction.
   b. CIS2 must be updated in accordance with the number reassignment.
   c. A memorandum documenting the reassignment must be placed in the file that receives the new A-number.
   d. The applicant receiving the new A-number must be notified of the need to reapply for their current status granting benefit and to request a fee waiver indicating service error.
   e. Notification procedures for affected individuals:
      i. At a minimum, two attempts to deliver a notice to the applicant's last known address must be made.
      ii. Notice must be sent through an approved delivery service using a return receipt. Undeliverable mail will be interfiled into the applicant's immigration record.
      iii. Offices will defer to local management discretion regarding any additional notification procedures.

6. If the resolution requires the assignment of a new A-number, the new number will be assigned according to the following hierarchy:
   a. The individual whose case is currently being adjudicated or investigated.
   b. If there is no current adjudication or investigation, or if each has a current adjudication or investigation; the individual whose information is the most current or the individual most easily contacted.
   c. The individual who has multiple files associated with his or her A-number.
   d. If both individuals are similarly situated, the individual with the later date of entry will receive the new A-number.

7. If a range of A-file numbers has been mis-assigned, notify BOIB at HQPCB-EM@uscis.dhs.gov.

Chapter 5 - Duplicate Certificate Numbers

1. Periodically, USCIS personnel may encounter the existence of duplicate naturalization certificate numbers. This occurs because the same naturalization certificate number is mistakenly attributed to multiple individuals ("true duplicate") or a previously issued naturalization certificate number is incorrectly entered into the CIS2.

2. If duplicate naturalization certificate numbers occur because the same certificate number has been electronically assigned to two individuals, field personnel should forward the cases to their local Adjudications unit for investigation and resolution. If the review shows that the duplicate certificate number was issued to two or more individuals and therefore considered to be a "true duplicate," Records personnel must correct the error in CIS2 and place a memorandum in the file describing the action that was taken to correct the error.

3. If duplicate certificate numbers are the result of incorrect data entry, Records personnel must correct the error in CIS2 and place a memorandum in the file describing the action that was taken to correct the error.

4. To correct the error in CIS2:
   a. Screen 9413 User Guide 4.16.4,
   b. Screen 9414 User Guide 4.16.5,
   c. Screen 9311 User Guide 4.15.6, and
   d. Screen 9312 User Guide 4.15.7.

5. Refer the cases to the Adjudications Unit for investigation and resolution.
   a. Upon completion of its review, the Adjudications Unit should return the cases to the Records personnel. Records personnel will update CIS2 with the new certificate number.
   b. Records personnel should follow steps outlined in paragraph 1 above in order to update CIS2 and the A-file.
   c. Enter the A-number of the file with the incorrect certificate number in CIS2 Screen 9413. If the record has a naturalization history, select the history and correct/delete the error.
   d. If the record does not have a naturalization history in CIS2 Screen 9413, delete the incorrect naturalization number using CIS2 Screen 9414.
   e. Next, correct the certificate number by using CIS2 screen 9311 or CIS2 screen 9312.
   f. Upon the updating of CIS2, Records Personnel should place a memorandum to the file describing the action that was taken to correct the error.

Chapter 6 - Record Consolidations, Combinations, and Disconnecting Consolidations

1. If there are multiple records on a person, take the records to the Records Unit and ask them to consolidate or combine the records.

2. Only Records personnel are allowed to consolidate, combine, and disconnect consolidated records.
   a. Records personnel must ensure that all information from the secondary file is placed in the primary file in ROP order.
   b. Records personnel must not rearrange the order unless specifically instructed by operations staff.
   c. Each ROP must be separated by a pink M-175 coversheet.

3. Consolidation
   a. Individuals should have only one record. Records must be consolidated (joining the contents of two or more records with different numbers but relating to the same individual) or combined when multiple records related to the same individual exist.
   b. When consolidating files, the primary record (surviving record) is the record into which other records are consolidated.
   c. The primary record contains the document with the higher action in the following hierarchy order: Adjudicators should reference their process guidance when in doubt.
      i. If a C-file exists for the subject, the C-file is primary.
      ii. If the subject has an A-number but no physical A-file, use the A-number to create a physical A-file and consolidate any historical files therein.

iii. If the subject has an historical record but neither an A-number nor a physical A-file, issue the subject a new A-number and consolidate any historical records into it.
iv. An approved application or petition or an issued certificate (for example, Form I-485, Application to Register Permanent Residence or Adjust Status; Form I-589, Application for Asylum and for Withholding of Removal; Form I-590, Registration for Classification as a Refugee; Form I-730, Refugee/Asylee Relative Petition).
v. Deportation, investigation, or other enforcement cases.
vi. Legalization records.
vii. If the records are of the same type, the oldest record is the primary.
viii. If the A-file is lost but the A-file number should be the primary number, follow the Files Lost During the Normal Course of Business procedures in RPM Vol 3, Part C, Chapter 9. At the end of that process, establish a sub-file on the primary number, and then consolidate the T-file or secondary file into the Sub-file. If subsequent documents are received on the secondary file, add the documents to a T-file and consolidate it with the Sub-file containing the primary number.
ix. If a missing A-file is located, the Substitute file is consolidated into the original A-file.

d. If there are multiple records to consolidate into one record, each record in the consolidation must be documented individually.
e. If it is determined that records relate to the same individual, the records must be consolidated by:
i. Determining the primary record;
ii. Correcting the record in CIS2 screen 9411 User Guide 4.16.2;
iii. Consolidating the physical records;
iv. Consolidating the electronic record in CIS2 screen 9402 User Guide 4.16.1;
v. Verifying consolidation in CIS2 screen 9101 User Guide 4.11.1;
vi. Consolidating (merging) in RAILS; and
vii. Destroying any secondary folders.

4. Screening
a. Review the entire record. One or two pieces of information are not enough to decide when files should be consolidated. The decision to consolidate should only be made after a thorough review and verification of the following items:
i. Names;
ii. Date of birth (DOB);
iii. Country of birth;
iv. Gender;
v. Parents' names;
vi. Fingerprints. (Do not use this as a sole determining factor);
vii. Certified documents;
viii. Photograph; and

ix. System Data. Check the information in CIS2 to make sure it matches what is in the physical file. It may be necessary to look at data in other systems (Treasury Enforcement Communications System/Non-Immigrant Information System (TECS II/NIIS), Arrival Departure Information System (ADIS), ENFORCE, Computer-Linked Application Information Management System (CLAIMS), et cetera.) to get additional identifying information. For example, CLAIMS and ADIS have address information; ENFORCE has deportation information, et cetera.

b. If there is no match, do not consolidate the records.

5. Correct the Central Index System 2 (CIS2), if needed
   a. If the secondary file contains a document with the higher action in the hierarchy, consolidate the secondary file into the primary file.
   b. Whichever number is referenced on the document is the record in CIS2 that should be updated. If you do not have a reference number then update the primary file number.

6. Electronically consolidating related records in CIS2
   a. After making the physical determination of which file is primary, consolidate the files in CIS2. Select the Consolidation of Records (XCON) Screen 9402. Only Records personnel can perform this function.
   b. Screen 9402 allows you to input information on as many records as needed using the following format:
      i. Enter the primary file first. In the first column, select "P" for the primary file.
      ii. In the next column, put in the A-number. Use only digits and start with zero.
      iii. Enter the secondary file next. In the first column, select "S" for secondary files.
      iv. In the next column, key in the A-number. Use only digits and start with zero.
      v. Repeat for each additional record.
      vi. When all the records have been entered, press enter.
      vii. After pressing enter, the next columns will show First Name, DOB, and FCO. Use this to resolve discrepancies. CIS2 will not accept the consolidation until the discrepancies have been resolved.
   c. Select the PF5 Key (or its equivalent) to access the online help system.

7. Physical consolidation
   a. Before implementing the physical consolidation, search RAILS to ensure there are no T or W files that may relate to the primary or secondary files.
   b. If records exist, request the records and make a final determination before proceeding with the physical consolidation. Take the material out of the secondary file and put it in the primary file. Follow these rules when moving documents from file to file:
      i. Separate each Record of Proceeding with a pink M-175 coversheet.
      ii. If it is a Legalization file (90,000,000-93,999,999 series), use a red M-330 to separate the ROP. If the M-330 is already in the file, you should use a pink M-175 to separate the ROP.

iii. Use Acco-style fasteners, not staples, to secure documents. If the documents are small, attach them to a piece of standard size paper and fasten it to the file.
iv. Place the most recent actions on top - reverse chronological order.
v. Place documents from the left side of the secondary folder on the left side of the primary folder. Do the same for the material on the right.

c. After moving the documents to the primary file, make a notation inside the left cover of the surviving jacket that includes:
   i. FCO;
   ii. Initials or employee number;
   iii. Date of the consolidation; and
   iv. The file number that was consolidated or combined.

8. Verify consolidation in CIS2
   a. Select the ID Number Search (ID) CIS 9101 in CIS2. Run a query on all the consolidated files and make sure the system recorded the information correctly. The primary file will show in bold letters.
   b. If CIS2 did not record the information properly, that is, the wrong record is the primary, follow the steps for the electronic portion of disconnecting the consolidation process.

9. Consolidating records in RAILS
   a. The process is not complete until the records are electronically consolidated in RAILS.
   b. Go to the main menu, select the "Merge" transaction and that will take you to the merge screen.
      i. Enter the primary (survivor) file number.
      ii. Enter the consolidated file number.
      iii. Select "merge".
   c. Select the RAILS Inquiry Screen to verify that the system made a successful consolidation. The screen will indicate file consolidation. To view the history, click on the history prompt or the consolidation key.

10. Destruction of secondary folders
    a. Blacken the label and barcode on the empty secondary file folders.
    b. Recycle or dispose of the empty folders.

11. Consolidating a Receipt file into an A-file, S-file, or T-file
    a. The steps in this consolidation are:
       i. Verify files relate;
       ii. Add Form M-175;
       iii. Annotate file jacket
       iv. Update RAILS; and
       v. Verify update in RAILS.

b. Verify that the two records relate. Check to ensure the identifying information such as A-number, name, date of birth, and country of birth match. If there is no match do not consolidate the records (see Section F-2, line 21 in this chapter for screening suggestions).
c. Place a pink M-175 on top of the documents in the primary file. Place the documents in the Receipt file on top of the M-175. Keep the documents in order. Fasten them to the left side, most recent record on top, with an Acco-type fastener. Do not staple documents to the A-file folder.
d. Annotate file jacket
e. Update RAILS
    i. Go to the main menu, select the "Merge" transaction and that will take you to the merge screen.
        - Enter the survivor file number.
        - Enter the consolidated file number.
        - Select "merge".
    ii. Do not delete the receipt files from the system. Anyone looking for them will be able to see the files were consolidated. If they are deleted, the local system does not indicate what happened to the file.
    iii. Select the RAILS inquiry screen to verify that the system made a successful consolidation.
    iv. Blacken the label and barcode of the Receipt files.
    v. Recycle or dispose of the empty folders.
f. If there are two of the same type of documents on the hierarchy list, refer the record to a Records Supervisor/Manager for resolution. The following considerations may helpful in determining which record should be designated as the primary file:
    i. Is this one of the files currently in adjudication or investigation?
    ii. Does one of the files contain a pending application or petition?
    iii. Are multiple files associated with one of the A-numbers?
g. A secondary file is a second file related to the same individual. Secondary files should be consolidated into the primary file.
h. Per policy memorandum Part II-03 dated March 5, 2019, A-file numbers between 80,000,000 and 86,899,999 (formerly "electronic only" numbers used to track Border Crossing Cards (BCC)) can now be created physically and added in RAILS. For A-numbers in this range with an enforcement or adjudicative action tied directly to it:
    i. FCOs must consolidate where an individual has a physical BCC file and a secondary A-number related to a physical file.
    ii. FCOs are not required to consolidate A-numbers in this range that remain tied only to BCCs.

12. Combination

a. This could be combining a sub-file, a temporary file, a work file/folder, or duplicate A-file into the original A-file.
b. Work folders generally contain documents non-record material such as rough notes, calculations, or drafts. These should not be combined into an A-file. However, if a work folder contains record material, then it must be combined into the A-file.
c. If two or more records have the same number, the records must be combined by:
    i. Determining the primary record;
    ii. Combining the physical records;
    iii. Combining (merging) records in RAILS; and
    iv. Recycling or destroying the secondary file folder.
d. RAILS does not use the same screen for consolidations (unlike suffixes) and combines (like suffixes). RAILS uses a process called combination to electronically combine the records.
e. Determine the primary file
    i. If there is an A-file, it is always the primary file. If there is not an A-file, but there is a Sub-file, the Sub-file is the primary file.
    ii. Verify the two records relate. Ensure the identifying information such as A-number, name, date of birth, and country of birth match. If there is no match do not consolidate the files.
    iii. If the records are of the same type, the oldest record is the primary. Move the most recent material onto the top of the material in the older file.
f. Physically combining records
    i. Be sure there is a pink M-175, Cover Sheet - Record of Processing, on the top of each record of proceeding.
    ii. From the secondary file, remove the documents and place them in the primary file in reverse chronological order – most recent documents on top. Place documents from the left on the left and documents from the right on the right. For more information, refer to the chapter entitled Record of Proceeding.
    iii. Small documents should be secured to a standard size sheet of paper and then fasten the paper to the file using Acco-type fasteners, do not staple materials to the A-file jacket. This applies to all small documents including post-it notes.
    iv. After moving the documents to the A-file, make a notation inside the left cover of the jacket that includes:
        - FCO;
        - Your initials or employee number;
        - Date of the combination; and
        - The file number that was combined.
    v. Attach any and all documentation (for example, bar code, history stamp) from the Sub-file to the interior of the A-file. Properly discard the remaining blank portions of the sub-file jacket.

g. Electronically combining records
   i. Before combining/consolidating, both files must be in the same Responsible Party Code (RPC).
   ii. If there is a Sub-file, please refer to Section S of this section.
   iii. In RAILS:
      - Select "Merge" from the main menu, and that will take you to the merge screen.
      - Select transaction "Combination".
      - Enter the Primary file number. Enter the secondary file number. Select merge.
      - Select the RAILS Inquiry Screen to verify that the system made a successful combination.

13. Who can consolidate, combine, and disconnect consolidated records
   a. Consolidations should not be initiated until someone from records has reviewed the files and verified that they are in fact the same person. These processes involve an electronic and a physical function. Only Records personnel can do both the electronic and physical processes.
   b. Program personnel are responsible for physical changes to the ROP. Records staff, unless authorized by program personnel, cannot change the ROP.
   c. If a program requests a consolidation and provides specific instructions for placement of materials within the ROP, then Records can perform the placement as instructed.

Personnel Responsibilities	Records Personnel	Program Personnel	Comments
Electronic processes	Yes	No	
Physical processes	Yes	Yes	
Documents from secondary gets into primary	Yes	No	
Rearranging order or determining placement	No	Yes	Records can do this with instruction from Program personnel

14. Disconnecting consolidations
   a. Disconnecting is the process of separating one record into two records.
   b. Consolidated files must be disconnected if the consolidated files do not relate to each other or the wrong file was designated as the primary.
   c. If the files do not relate to each other or the wrong record was designated as the primary, you must
      i. Disconnect in CIS2 screen 9402 User Guide 4.16.1;

- Key in "D" for disconnect and list the Primary file.
- Key in "D" for disconnect and list the secondary file.
- Repeat if there are more secondary files.
- Be sure to list all the secondary files or the system will not accept the disconnect.
- The system will give you a prompt letting you know it has disconnected the files.

ii. Physically separate the material into the new A-file jacket (with the number and barcode) for the disconnected record.
iii. Notate inside the left cover of the jacket the A-file number that was disconnected, the FCO, initials or employee number, and the date of deconsolidation.
iv. Verify the deconsolidation in RAILS. Once the primary file is in transit, you cannot disconnect a consolidation.

d. If the wrong record was designated as the primary, select the Consolidation of Records (XCON) Screen 9402 to deconsolidate.
i. Key in "D" for disconnect and list the primary file.
ii. Key in "D" for disconnect and list the secondary file.
iii. Repeat for each secondary file if there is more than one.
iv. Be sure to list all the secondary files or the system will not accept the disconnect.
v. The system will give you a prompt letting you know it has disconnected the files.
vi. Next, change the information in RAILS. Once the primary file is in transit, you cannot disconnect a consolidation.
vii. Replace the folder label with a new label showing the correct primary number and barcode.
viii. Next, repeat the consolidations steps, designating the proper file as primary.
ix. Physically separate the materials. After moving the documents to the primary file, make a notation inside the left cover of the jacket that includes:
- The file number that was disconnected;
- The FCO;
- Initials or employee number;
- The date the consolidation was disconnected; and
- Annotate the change in the primary and secondary files.

15. Post-consolidation or combination record maintenance
a. After consolidating or combining records, use only the primary number when creating new documents. Do not create new documentation using the secondary numbers.
b. Make CIS2 updates using only the primary number. Do not update any of the information for the secondary number.

16. Combining Sub-files
a. Physical combination

i. Combine the Sub-file material with the A-file in ROP order.
ii. Annotate the inner left side of the original A-file folder with the following:
- Action taken;
- FCO;
- Date; and
- Signature.

iii. Attach any and all documentation (for example, bar code, history stamp) from the Sub-file to the interior of the A-file. Properly discard the remaining blank portion of the Sub-file jacket.

b. Electronic combination
i. The electronic combining process is slightly different when combining a Sub-file and an A-file. Sub-files and A-files must have suffixes.
ii. Electronically combine the Sub-file with the A-file using CIS2 Screen 9403. Enter "M" (merge) to identify the merger of the Sub-file and the A-file. The merger should be verified by using CIS2 Screen 9101.
iii. Update RAILS to reflect the merger of the Sub-file and the A-file by using the Combine Files transaction

c. RAILS does not allow an A-file to be electronically consolidated into a Sub-file. If a Sub-file must be consolidated into an A-file, enter a comment in RAILS explaining the consolidation.

17. Combining T-files
a. Combine the T-file with its corresponding A-file or S-file.
b. The FCO holding the T-file must send the T-file to the FCO holding the A-file when action is complete or no longer needed, except for the NRC.
c. The FCO holding multiple T-files must combine them with the A-file as soon as possible when action is complete or when the T-file is no longer needed (except the NRC which combines T-files on request). See RPM Vol 3, Part C, Chapter 6.
d. FCOs must coordinate between offices to accomplish A-file and T-file (T-file and T-file) combination.
e. Do not send T-files to the NRC if the corresponding A-file is not located at the NRC. View the NRC Customer Guide for more information.

18. Conditions for consolidation of historical records
a. Whenever an individual with an inactive case (one that has been adjudicated or processed as far as possible) reenters the immigration process (such as when a new application for a benefit is submitted by the individual or an investigation proceeding is instituted against them), their case again becomes active. Any additional historical files relating to the subject that are identified should be consolidated with the primary A-file or Certificate files (C-file).
i. C-files

- All files, including any A-file, must be consolidated in the C-file.
- Only if the subject has expatriated shall the C-file be consolidated with the A-file.

ii. Consolidating A-files: If no C-file exists for the subject, all relating files shall be consolidated with the A-file.

b. If the case is not active, do not issue an A-number, create an A-file, or consolidate files.
c. For more information regarding file consolidation, See RPM Vol 3, Part C, Chapter 6.
d. To consolidate or deconsolidate a digitized EDMS file with a non-digitized file
   i. Send the request to the NRC Soda Team mailbox, SODATEAM.NRC@uscis.dhs.gov
   ii. The subject line must read: Request for File Consolidation or File Deconsolidation
   iii. The body of the email message must include the following information:
   iv. Reason for the request (to include designation of primary and secondary records for consolidation);
   v. A-numbers to be consolidated or deconsolidated;
   vi. Name/Location of the requester (Agency/FCO or Sub-Office Code);
   vii. Telephone and Fax number of the requestor; and
   viii. Email address of the requestor.
e. It may be necessary to provide supporting documentation that will attest to the requested change of information. This is done to prevent fraud and to ensure the integrity of the record.
f. If both files have been digitized, consolidated can be done locally. Please review EDMS first to ensure you are consolidating the correct files. Key data elements must be updated in RAILS before you consolidate files. A comment must be added to RAILS for the files you have consolidated.

19. Records at the Federal Records Center
   a. The Federal Records Center (FRC) is part of the National Archives and Records Administration (NARA). Records at the FRC still belong to DHS but are in the care of the NARA.
   b. If there are records that need to be combined with a record retired at the FRC, have the record pulled:
      i. If the requesting FCO retired the record, call or email the Records Unit and ask them to request the record. Provide the A-number and contact information.
      ii. If another FCO retired the file, request the file just as you would for any other record in another FCO.
   c. For more information about retired records, see RPM Vol 3, Part G, Chapter 2.

Chapter 7 - Handling Damaged or Contaminated Records

1. Upon discovery of contaminated records, the priority is always the safety and health of the personnel who handle the records and you must notify a supervisor.

2. The supervisor must immediately generate a SIR upon discovery of contaminated records and notify the following:
   a. The Collateral Duty Safety Officer (CDSO); and
   b. The Office of Security and Integrity (OSI) Field Security Manager (FSM).
   c. Consult the Field Security Manager and Local Security Officer Contact List for points of contact.
3. If classified information is involved, the CDSO must also complete DHS Form 11000-10, Report of Security Incident, (Record of Security Violation). The OSI Security Handbook provides instructions for completing this form.
4. After consultation with OSI, the office should contact a professional restoration service to handle the material.
5. In cases where large numbers of files (for example. 100 or more files) are involved, there is a complex or unknown situation, or suspected hazardous materials may be present, the supervisor must also notify the USCIS Chief of Emergency Management and Safety, the Designated Agency Safety and Official (DOSHA) for USCIS.
6. ICE and CBP offices must notify their local USCIS Records unit.
7. Offices may contact the OSI Emergency Management and OSI Occupational Safety and Health Branch for assistance at any time.
8. Overview
   a. Exposure to excessive moisture is the most common cause of damage to immigration records and, if unaddressed, may lead to contamination by mold and mildew.
   b. Contamination of records occurs with exposure to substances such as chemicals, blood, mold, and insect/animal feces. Contaminated records usually fall into one of the following categories:
      i. Non-hazardous substance such as water, dust, dirt, food product, or insects;
      ii. Chemical contamination such as insecticide, asbestos, cleaning fluids, or other chemicals;
      iii. Biologic contamination such as blood/body fluids, anthrax, sewage, or mold; or
      iv. Mixed contamination such as records exposed during flooding due to a combination of sewage and chemical contaminants in the water.
   c. For guidance on mechanically damaged files such as those torn, abraded, or ripped, see RPM Vol 3, Part C, Chapter 7
9. Procedures for handling water damaged records
   a. The employee discovering files possibly damaged by water should immediately notify a supervisor. The supervisor should contact the CDSO.
   b. The supervisor should clear the area and isolate the record.
   c. A situation may be classified as a minor wetting event if:
      i. The wetting agent is positively identified as tap water, rain water or sprinkler water (not sewer water or other potentially contaminated source).

ii. Conditions have not been extremely hot and humid.
iii. Records have been wet for less than 24 hours.
iv. Number of records is limited and can be air dried within 48 hours.

d. If it is determined that the situation is a minor wetting event and there is no threat of contamination:
   i. Carefully separate documents and lay them on a non-solid surface through which air can pass underneath (that is wire mesh, wooden pallets, et cetera);
   ii. Set up fans to circulate air. Do not aim directly at documents and use small objects as paperweights if necessary;
   iii. Turn documents over as necessary to dry evenly;
   iv. Take care to ensure that PII is protected from unauthorized access, and
   v. Reassemble record(s) when dry.
e. If there is water damage that the local office cannot handle, generate a SIR. The CDSO must complete an assessment of the situation to include the following information:
   i. Identification of the damage (that is, water, fire, unknown substance);
   ii. Is there an immediate risk to personnel;
   iii. How many files have been damaged;
   iv. Level of damage to the files;
   v. Potential threat from exposure (if any);
   vi. Is there any contamination (if known);
   vii. Should the damaged file(s) be moved; and
   viii. Does the situation warrant activating local emergency plans (OEP, etc.).
f. Files exposed to moisture may become contaminated by mold or mildew. If mold, mildew, or other contaminants appear to be present, please follow the procedures for handling contaminated record(s).

10. Procedures for handling contaminated records
   a. Where there is an unknown substance, employees should not handle records until determined safe to do so by a CDSO or other approved authority.
   b. The employee discovering possibly contaminated records must immediately notify a supervisor. The supervisor must contact the CDSO and OSI Field Security representative. The supervisor should also attempt to identify any personnel who potentially handled the records.
   c. If classified information is involved, complete DHS Form 11000-10, Report of Security Incident, (Record of Security Violation). The OSI Security Handbook provides instructions for completing this form.
   d. The CDSO must complete an assessment of the situation including the following information:
      i. How many records have been contaminated;
      ii. Level of contamination to the records;
      iii. Potential threat from exposure (if any);
      iv. Type of contamination (if known); and

v. Should the contaminated record(s) be moved?

e. The CDSO should examine the circumstances surrounding the contamination to determine its source. Determination of the source will assist in understanding the nature of the substance and its level of concern.

f. If a record(s) appears to be contaminated by mold or any other unknown substances that may pose a risk to personnel, take the following steps:
   i. Cease handling of the file(s), attempting not to disturb or cause further contamination. Do not place contaminated records into plastic bags.
   ii. Isolate the affected record(s) and evacuate the immediate area. In the absence of a clear threat such as a written note, telephone threat, or increased security related to intelligence; unknown substances should be treated as unknowns and not as suspicious substances. The employee/contractor should clear the immediate work area and notify a government supervisor to evaluate the situation.
   iii. The File Control Office (FCO) in consultation with OSI and others will determine if the situation needs to be elevated or if additional notifications are necessary.

11. Coordination with OSI
   a. If the material is contaminated, coordinate with OSI or the CDSO to identify an approved professional hazardous materials service.
   b. When management of the contamination goes beyond the capabilities of the local office, notify the Emergency Management and Safety Office at OSISecurityOperations@uscis.dhs.gov.

12. Other considerations
   a. Offices should develop local procedures to address the following operational issues:
      i. Creation of an inventory of the records affected;
      ii. Review of systems (that is, CIS2/C4/CLAIMS) to see if there are open applications/interviews pending or if outstanding file requests exist; and
      iii. If needed, creation of a separate RAILS code for the affected records and their tracking.
   b. For additional information on please see National Archives and Records Administration Records site on Recovery, Records Emergency Disposal, and Information Security.

Chapter 8 - Working with Records Outside of Government Worksites

1. Introduction
   a. This section describes how to properly safeguard sensitive immigration records in the custody of a DHS employee who is not working at a government worksite. It pertains to all sensitive records taken offsite including telecommuting sites.
   b. This section does not apply to classified files.
   c. This section does not pertain to records in transit between different government worksites.

2. Privacy Act overview

a. Most sensitive records are subject to the Privacy Act. The law requires certain safeguards for these types of records. These safeguards apply wherever you work – in a government office, at home, or on travel.
b. Any record that contains information about an individual immigrant or citizen is subject to the Privacy Act.
    i. Each system of records subject to the Privacy Act must have a Systems Notice.
    ii. This System Notice lets the public know what records are kept and how they are kept by publishing the information in the Federal Register.
    iii. Before approving off-site use of sensitive records, supervisors must ensure the Privacy Act Notice for that set of files allows off-site use.
        - The FOIA/PA handbook lists all the Privacy Act Notices for immigration records.
        - Check the Safeguards section of the Privacy Act Notice.
    iv. Examples of types of files subject to the Privacy Act are:
        - A-files;
        - Personnel files;
        - Security investigative files; and
        - Receipt files pertaining to immigrants.
    v. Nonimmigrant records are not subject to the provisions of the Privacy Act. However, all records with personal information need to be adequately safeguarded.

3. Permission to take sensitive immigration records requires a written agreement and must come through your supervisory channels.

4. People who need to work with sensitive records outside a government facility but do not have a telecommuting agreement, for example, people who are on travel or investigators, must have their supervisor's approval to take sensitive records out of the worksite.

5. Classified records cannot be removed from official worksites to off-site locations.

6. Employees must follow the DHS Handbook for Safeguarding Sensitive PII.
    a. When transporting records from the office to another location, keep sensitive property and information in your possession unless locked in a cargo/luggage compartment, the contents of which are not visible from outside the conveyance.
    b. Work on records in an area that prevents access and casual observation by unauthorized people (this includes family members).
    c. Secure records in a locked room or locked cabinet when not in use.

7. Supervisor responsibilities for employees taking sensitive records off-site:
    a. Provide written approval;
    b. Assign a specific telecommuting Responsible Party Code (RPC);
    c. Verify that the employee's list includes all records removed from the worksite;
    d. Verify that records are properly charged out/assigned in RAILS;

e. Ensure the records can be returned within 4 hours or within the time required by your office if needed;
f. Ensure the records will be properly safeguarded from theft, loss, and unauthorized disclosure;
g. Report any lost or missing records to the supervisor of the Records Unit;
h. Maintain information on how to contact the employee with the records; and
i. Reconcile the records assigned to the employee on a monthly basis.
j. If there is a request for a record and the record is off-site:
    i. Let the supervisor of the Records Unit know who has the record;
    ii. Contact the employee with the record and find out when the record can be returned; and
    iii. If the record cannot be returned, inform the supervisor of the Records Unit so the record can be updated with In Use in RALIS.

8. Employee responsibilities for taking sensitive records off-site:
    a. Obtain written permission from your supervisor;
    b. Verifying that you have all records assigned to your telecommuting RPC;
    c. Provide a list of all files in your possession to your supervisor;
    d. If you do not have one of the records assigned to your telecommuting RPC, report it to your supervisor;
    e. Upon return to the office, immediately return all immigration records in your telecommuting RPC;
    f. Provide your supervisor with a phone number and location where you can be reached;
    g. Ensure you can return records to the office within 4 hours (or the time required by your supervisor) if there is an emergency;
    h. Advise your supervisor what arrangements you have made to have the records returned to the worksite in the event of an emergency, such as an illness or accident that would preclude you from returning the file in a timely manner.

9. Report any loss, theft, or significant damage to records immediately. Notify your supervisor, the Security Officer, and the Records Supervisor.

10. Records Supervisor responsibilities
    a. The local records office is responsible for keeping track of the records in your local RAILS system. If employees take other types of sensitive records out of the office, the Records Office is involved only when files are lost or destroyed.
    b. When doing monthly audits, ensure you include all records in RAILS, even those charged out to telecommuters or others who use the records off-site.
    c. Supervisors of employees who use records outside government worksites are to report any lost, missing, or damaged records to you. Update RAILS appropriately and follow the procedures for dealing with lost or damaged records.

d. When an employee working off-site for a reason other than telecommuting takes records for more than three days, their unit supervisor will provide you with a list of the records taken.
e. When there is an FTR pending for records taken off-site, coordinate with the unit supervisor of the person with the record to either obtain the record or update RAILS with In Use.

Chapter 9 - Records Lost and Missing from the Office

1. Primary causes of missing records
   a. Missing/lost files misplaced prior to April 18, 2016 are exempt from the requirements set forth in this policy. For missing or lost records prior to April 18, 2016, follow the lost file recovery plan implemented during the time period.
   b. A record is missing when:
      i. The record is physically moved, but the movement is not recorded or not correctly recorded in RAILS, and there is no evidence that it has been lost. Therefore, it is assumed to remain within the government's control. Record movement means: any physical movement of a record from one Responsible Party Code (RPC) location to another RPC location, whether or not shipping is involved. This includes movement from one individual to another, movement within a File Control Office (FCO), and movement between FCOs.
      ii. The record is physically consolidated, but the electronic consolidation in RAILS is not completed.
      iii. During a record audit when Unaudited Files Report is generated and reconciled, and the record still cannot be located.

2. Special searches for missing records
   a. Perform a special search each time you cannot locate an immigration record.
   b. Complete the special search steps outlined below in sequence. If at any point during the search you find the record, send it the requester, if applicable.
   c. Search all the records in the RPC the file is currently assigned to, the last previous assigned RPC, and all surrounding RPCs. The following steps are recommended (this is not an exhaustive list):
      i. Check the history of the file in RAILS. Look for the previous locations and check them. If the record was in an operational unit, check the unit's inbox and outbox.
      ii. For Shelving RPCs, check the RPCs on each side and the ones above and below the assigned RPC.
      iii. Check the RPCs based on your local FCO workflow, including but not limited to the following areas:
         - Shipping to other offices or the National Records Center (NRC);
         - Refiling; and

- Determining where in the local workflow process the file may have been sent based on form type(s). Confirm with the RPC owner that they do not have the file regardless of whether it was sent internally using RAILS

iv. Check barcodes of surrounding records to ensure that the front and back barcode match.

d. CIS2 FTD screen accessed by selecting PF11 from the 9504 screen is no longer updated with record location and status information. The CIS2 FTD data froze on the date CIS2 deployed but will be available to CIS2 users to query for historical purposes.
   i. If the FCO does not match, contact the previous FCO and ask if they have the record.
   ii. If the previous FCO has the record, update RAILS using the Send transaction (In RAILS, the previous FCO must "Receive" the record). Work with the FCO to update the system.
   iii. Perform a name search in CIS2. Check any related records for possible consolidation of these records.

e. If your FCO code is commonly confused with anther FCO, contact the other FCO. If the other FCO has the record, arrange to have the FCO transfer the file. Examples include:
   i. "NEW" is the code for Newark but commonly mistaken for New York;
   ii. "WAS" is the code for Washington District Office but commonly mistaken for Headquarters; and
   iii. "COW" is the code for Headquarters but commonly mistaken for Washington District Office.

f. Check Federal Records Center (FRC) docket cards:
   i. Before the implementation of the Receipt and Alien File Accountability and Control System (RAFACS), offices used FRC docket cards to record the transfer of files to the FRC.
   ii. Docket cards are in terminal digit order.

g. Check other systems, including USCIS Case Management Systems (such as CLAIMS and ELIS) and enforcement systems using PCQS.

3. Documenting missing records
   a. After performing the required special search and confirming that a record is missing (Note: For files sent between RPCs within your FCO, allow 7 days for the file to be received), update the file in RAILS using the Missing Internal File transaction (do not change RPC).
      i. This process must be completed by an individual with the Missing User Role in RAILS. This User Role is obtained by submitting a request in MyAccess. The User Role should be restricted to records staff and supervisors.
      ii. The Missing Internal File process in RAILS will require users to respond to the following questions;

- For in transit files, the intended recipient or owner of the receiving RPC has been contacted and after a special search was conducted has confirmed that they do not have physical possession of the file.
- A special search of the original RPC was conducted in accordance with applicable policy contained within the RPM and the file could not be located.
- I have confirmed that there is no evidence that the file in question has fallen outside of government control and there is no evidence of a loss of personally identifiable information.
- I hereby certify that all requirements listed in the Records Policy Manual for marking files missing have been completed.

iii. RAILS tracks the completion of the missing internal file process under the Missing File status entry in the file's history. This entry serves as an attestation that the FCO has completed all policy requirements for the missing file. It does not state that the individual marking the file has personally performed each step. FCOs may retain information of local employees' completion of individual process steps as part of a local SOP.

b. If a missing record is in the custody of ICE or CBP, USCIS must complete Missing Internal File process in RAILS. However, ICE or CBP is responsible for the incident response and mitigation duties.

c. Create a Substitute file or Temporary file as appropriate. If an office determines that a Substitute file is needed for a business requirement (requested for agency business, such as adjudication, retirement, or enforcement-related actions), it should wait 60 working days from the date the record was updated to Missing before creating a Sub-file.

4. Lost during normal course of business

a. A record is lost when USCIS can "verify" that the record was not received in transit, has been destroyed, or is not verifiably under U.S. government control.

b. Though records are normally under government control during the normal course of business, there is a possibility that records may be moved outside the secured areas and then lost.

c. All lost records require a SIR to be filed. A copy of the SIR must be sent to IIMD at HQPCB-EM@uscis.dhs.gov and the USCIS Records Officer at USCISRecordOfficer@uscis.dhs.gov.

d. After performing all required searches and confirming that a record is lost and filing a SIR, update the file in RAILS using the Lost Internal File transaction (do not change RPC).

i. This process must be completed by an individual with the Lost User Role in RAILS. This User Role is obtained by submitting a request in MyAccess. The User Role should be restricted to records staff and supervisors.

ii. A SIR Number must be entered in the system for each file being marked lost at time of initial file number entry.

iii. The Lost Internal File process in RAILS will require users to respond to the following questions;
- The files in question:
  - Cannot be found after being exposed to an area outside of government control and the PII they contain may have become accessible to unauthorized individuals; or
  - Were destroyed within the Agency.
- For internally in transit files, the intended recipient or owner of the receiving RPC has been contacted and after a special search was conducted has confirmed that they do not have physical possession of the file.
- A special search of the original RPC was conducted in accordance with applicable policy contained within the RPM and the file could not be located.
- I hereby certify that all requirements listed in the Records Policy Manual for marking files missing have been completed.

iv. RAILS tracks the completion of the lost internal file process under the Lost File status entry in the file's history. This entry serves as an attestation that the FCO has completed all policy requirements for the lost file. It does not state that the individual marking the file has personally performed each step. FCOs may retain information of local employees' completion of individual process steps as part of a local SOP.

5. Records missing or lost during telework
   a. If records taken away from the worksite cannot be located, conduct a search of the telework site (and surrounding areas, if applicable) immediately upon discovery.
   b. If a missing record is not found after a search of the telework site:
      i. Report the loss to a supervisor;
      ii. Complete the Missing Internal File process in RAILS (do not change RPC); and
      iii. Create a Substitute file or Temporary file as appropriate. If an office determines that a substitute file is necessary, it should wait 60 working days from the loss of the file before requesting approval for record creation.
   c. Records can be lost during telework if the record is known to be destroyed or out of the employee's control (for example, their car is stolen with records in the trunk, or there is a house fire).
   d. If a record is lost during telework, complete the Lost Internal File process in RAILS and complete a SIR.

6. Classified and National Security Files additional requirements
   a. In addition to the regular missing or lost process, Classified and National Security Files require the completion of a DHS Form 11000-10, Record of Security Violation in accordance with OSI procedures. This form must be completed and emailed to IIMD mailbox, HQPCB-EM@uscis.dhs.gov with Missing or Lost File, as applicable, in the subject line.

7. RAILS records that are marked as missing or lost are automatically moved by the system to one of the following missing or lost RPCs after 90 days, as appropriate for each DHS component:
   a. Missing:
      i. ZY0914-USCIS
      ii. ZY0915-ICE
      iii. ZY0916-CBP
   b. Lost:
      i. ZY0911-USCIS
      ii. ZY912-ICE
      iii. ZY0913-CBP
   c. These ZY codes are system managed and must not be manually used.
      i. Users must not move records into these codes.*

         *Exception: RAILS does not allow deactivation of RPCs currently holding files. If an office must deactivate an RPC that contains lost or missing files, those files can be moved manually to the appropriate ZY code. Manual file movement into ZY Codes shall only occur when RPC deactivation is necessary.

      ii. Users shall not remove records from these codes unless the lost or missing record has been found.

Chapter 10 - Records Lost and Missing from Transit

1. Overview
   a. Offices are not required to follow the following procedures set in this policy and complete a Missing Checklist or Significant Incident Report (if applicable) for missing/lost records misplaced prior to April 18, 2016. For missing or lost records prior to April 18, 2016, follow the lost record recovery plan implemented during the time period.
   b. An immigration record is lost when USCIS can "verify" that the record was not received after transit, has been destroyed, or is not verifiably under U.S. Government Control.
   c. An immigration record is missing when:
      i. The record is moved, but the movement is not recorded or not correctly recorded in RAILS, and there is no evidence that it has been lost. Therefore, it is assumed to remain within the government's control. File "movement" means: any transfer of a file from one Responsible Party Code (RPC) to another RPC code, whether or not shipping is involved. This includes movement from one individual to another, movement within a File Control Office (FCO), and movement between FCOs.
      ii. The record is physically consolidated, but the electronic consolidation in RAILS is not completed. For example, a denied I-90 that was consolidated into the corresponding A-file but the consolidation was not recorded in RAILS.

iii. A record is sent internally from one RPC to another but does not arrive at the destination.

d. When an FCO determines that the record is missing they will need to complete a mandatory checklist, either a Missing Internal File Checklist or the Missing External File Checklist.

e. A sending office must alert the intended receiving office if a record in transit externally has not been transferred into the receiving office through RAILS after 16 working days. Exceptions include the following:
   i. If sending a record(s) to the National Records Center (NRC) or the Remote File and Maintenance Facility at Harrisonburg, Virginia (HBG), the sending office must alert the intended receiving office if the record(s) has not been transferred in through RAILS after 30 working days.
   ii. If sending a record(s) overseas, the sending office must alert the intended receiving office if the record(s) has not been transferred in through RAILS after 45 working days.

f. Once verified that neither office has the record because the shipment was lost or destroyed, the sending office must initiate the Lost File Checklist.

g. The FCO's Records Supervisor, Manager, or Specialist should maintain the Lost Files Checklist for one year after the completion of the OSI investigation. Email a copy to IIMD at HQPCB-EM@uscis.dhs.gov.

2. Sending office procedures with no documentation of delivery
   a. Once it is verified that a record(s) is not located in the sending or receiving offices, the sending office will contact the carrier to:
      i. Provide the tracking number(s), if available, to the carrier to facilitate the investigation; and
      ii. Request documentation from the carrier that the package was properly handled by the carrier.
   b. If the carrier provides documentation that the shipment is lost*, the record(s) are considered lost and the sending office must follow the procedures below:
      i. Initiate the Lost File Checklist.
      ii. Complete a Significant Incidence Report (SIR) within one hour in accordance with OSI procedures. Send a copy of the SIR to OSI at uscis.c2@uscis.dhs.gov and to IIMD at HQPCB-EM@uscis.dhs.gov. When sending personally identifiable information (PII), use an approved email encryption method to protect the documents you wish to email.
      iii. If the lost file(s) is/are classified, a DHS Form 11000-10, Report of Security Incident, (Record of Security Violation) must also be filed.
      iv. Place a memo, identifying the SIR number sent to OSI, in a Sub-file or Temporary (T) file. If an office determines that a Substitute file is necessary, it should wait 60 working days from the loss of the file before requesting approval for file creation.
      v. Update RAILS with the proper status code depending on results of special searches.

c. *NOTE: If the carrier does not provide any documentation regarding the delivery of the shipment, it is considered missing.

3. Sending and receiving office procedures with confirmed delivery
   a. If the carrier provides documentation that the shipment was delivered, the sending office must follow the procedures below
      i. Contact the receiving office (in writing) and advise them that they are now responsible for completing the remainder of the Missing External File Checklist (Steps 3 through 5).
      ii. NOTE: If additional information is obtained while completing a Missing External File Checklist that indicate the record(s) are actually lost, shred the Missing File checklist and complete a Lost File Checklist.
      iii. Provide the receiving office with a copy of the checklist with Steps 1 and 2 completed and a copy of the document showing delivery of the file(s) by the carrier within 10 business days. The sending office's portion of the File Checklist is complete at this point.
      iv. Perform all system updates regarding the missing file until the file is located:
      v. Update RAILS with the proper status code depending on results of special searches.
   b. Upon receipt of the Missing External File Checklist, the receiving office must conduct a special search.
   c. If the file cannot be found after completion of special searches in the receiving office, the receiving office must follow the procedures below.
      i. Complete the remaining portion of the Missing External File Checklist and retain a copy in your office for one year.
      ii. If the lost or missing record(s) is/are classified, file a Security Violations Form (SVR) (DHS Form 1110-10).
      iii. For classified records, place a memo, identifying the SVR number sent to OSI, in a Sub-file or Temporary (T) file. If an office determines that a Substitute file is necessary, it should wait 60 working days from the loss of the record before requesting approval for record creation.
      iv. If an office determines that a Substitute file is necessary, it should wait 60 working days from the loss of the record before requesting approval for the record creation.

4. Records Security Overview
   a. Even though most of the information the DHS collects as part of enforcing immigration law is not classified, it is sensitive. It is important to properly safeguard both electronic and hardcopy information.
   b. These rules apply to unclassified material; there are more stringent requirements for handling classified files.

5. Everyone working for the DHS is responsible for properly protecting the information stored in A-files or DHS systems. A-files are part of the Privacy Act System of Records and as such, must be protected against unwarranted invasion of the privacy of the person to whom the file pertains.
6. Review Chapters 7 and 8 of the Security Officer's Handbook. These chapters explain the security requirements for storing both classified and non-classified materials.
7. File rooms
   a. Store A-files only in rooms or offices with adequate physical access protection against unauthorized access by members of the public and visitors such as a locked room or an area where access is controlled by a cipher lock or card reader.
   b. Store supplies in a separate area under separate control.
   c. Question unauthorized access to files at any time or in any situation. In general, only people assigned to the Records Unit should access the file room. If you notice an unfamiliar person in the file room
      i. Ask if you may assist them;
      ii. If they are not part of the Records Unit, let them know they should not be in the files area; and
      iii. Report the incident to your Records Unit supervisor.
8. Securing records in other work spaces
   a. When unattended, A-files will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment.
   b. A-files can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.
9. Records supervisor's responsibilities
   The Records Supervisor should:
   a. Establish local procedures to enforce the guidelines provided above.
   b. Ensure records employees are trained to know their security responsibilities and how to fulfill them.
   c. Ensure employees have the appropriate systems access level for their duties, responsibilities, and clearance. Review access regularly.
   d. Have a departing employee's system access deleted.
   e. Delete or downgrade system access when an employee no longer is authorized access or no longer needs it.
10. Reporting incidents
    a. Reportable incidents include:
       i. Detection of computer viruses;

ii. Access by people without proper credentials;
iii. Bypassing of physical access controls (locks and guards);
iv. Unauthorized access to computers, systems, or applications;
v. Unauthorized alteration, destruction, or disclosure of data or records;
vi. Damage to government owned property or records;
vii. Loss, theft, or abuse of computer resources;
viii. Power and telecommunications outages;
ix. Unexpected system crashes or poor system performance; and
x. Misuse by another user is discovered such as inappropriate use of email or the Internet, unauthorized or unlicensed use of software, or sharing of passwords.

b. Report all incidents to your local Computer Systems Security Office (CSSO). Contact your help desk if you do not know who is the local CSSO.
c. If the incident involves files, report it to the supervisor of the Records Unit as well.

Chapter 11 - Auditing Records

1. The record audit process checks to ensure the physical location of the record is properly recorded in the electronic tracking systems. This audit process applies to all ACTIVE files. For files tracked by RAILS, the audit process compares the physical location to the electronic location. If there is a discrepancy, the system is updated and a report is generated. For RAILS, the system provides discrepancy information directly on the screen. From there, the user can directly reconcile the discrepancies or print the list.

2. All FCOs must audit their records and conduct reconciliation at least once per fiscal year with the following exceptions:
   a. The NRC is required to complete an audit of all records once every 5 years.
   b. Harrisonburg is exempt from performing annual audits.
   c. Service contracts may have additional audit requirements.
   d. Records containing classified information and empty jackets must be audited twice a year (within 183 days).
   e. RAIO and SCOPS have a five-year exemption for backlogged files stored with outside file-storage vendor.

3. All FCOs must run their “unaudited files” SMART report at the start of each fiscal year (October 1) and have until the end of the same fiscal year (September 30) to conduct the audit and reconcile the October unaudited report.

4. Auditing records once a year is the minimum requirement; FCOs may and are highly encouraged to continue to conduct rolling audits, quarterly audits, or other local procedures as long as they are complete by September 30th.

5. Audits must include all RPCs, sub-offices, operating units, and other offices under the jurisdiction of the FCO. Each FCO must maintain either a digital or paper audit record. This record must keep track of fully audited RPC or Terminal Digit Order (TDO) [optional] sections. The audit record must include:

a. The RPC or TDO (Optional) sections audited;
b. The audit date; and
c. The name of the auditor.

6. In order for the audit to be complete, the unaudited reports must be reconciled (preferably the same day).
   a. In RAILS, unaudited file information is available on screen. From there it can be directly reconciled or printed for review
   b. Check the report/on screen RAILS information to review and correct the audit findings.
   c. Run the unaudited files report.
   d. Follow the RAILS procedures for uploading the data.
   e. If after 14 days from the audit date an office has files that remain unreconciled, RAILS will generate a notification to the records manager and supervisor for the applicable RPCs. This message states that there are files that remain unaudited and have not been moved to a Missing or Lost status.

7. All classified physical files must be conducted semi-annually with no more than 183 days in between each audit, and reconciliation of classified physical must include:
   a. File Control Offices (FCOs) will conduct semiannual audits in RAILS to ensure accurate accountability, conduct a physical inventory audit, and reconcile all empty A-file jacket and classified file inventory.
      i. The time period between audits cannot exceed 183 days (for example, at the end of the 2nd and 4th quarters).
      ii. Audits must include all sub-offices, operating units, and other offices under the jurisdiction of the FCO.
      iii. Regional Offices have the discretion to allow ICE or CBP staff to conduct physical audits for files located within ICE and CBP offices that are not co-located. Please note that accountability remains at all times with the Regional Offices.
      iv. NOTE: Records exceeding 183 days are considered to be noncompliant. FCOs have the option to conduct as many audits as preferred within the indicated time frame.
   b. Review to ensure markings and cover sheets are affixed to each file;
   c. Reconciliation of Unaudited Report;
   d. Conducting the "Reporting" process through the Security Office. Report as required by Office of Security and Integrity (OSI). Submit written notification to the Field Security Manager (FSM) and complete DHS Form 11000-10, Report of Security Incident, (Record of Security Violation). In accordance with 32 CFR 2001.48 any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose. Per USCIS Security Handbook Chapter 8, Part F, Item 2.2, classified audits must be reconciled immediately; and

e. Administering Significant Violation Report and Missing/Lost File Checklist to IIMD. Any classified physical files not found during the reconciliation must be processed in accordance with RPM Vol 3, Part C, Chapter 9 and RPM Vol 3, Part C, Chapter 10.

8. The EJM is responsible for conducting audits, recording audit results, and reporting audit results of empty A-file jackets to directorate Records POC.
   a. FCOs holding limited quantities of empty A-file jackets must manually scan each individual empty A-file jacket to satisfy the semiannual audit requirement. The FCOs must provide their semiannual audit reports through their chains of command (for example, field offices would provide their reports to their regional offices).
   b. An FCO holding large quantities of empty A-file jackets has the option of verifying their empty A-file jacket audit using Form G-1191, Empty A-File Jacket Audit Results.
      i. The FCO will submit Form G-1191 through their chain of command; and
      ii. The office authorized to control distribution will then submit the G-1191 form to HQPCB-EM@uscis.dhs.gov.
   c. Offices must maintain the audit records in an Office Administration File (General Records Schedule 23-1) unless it relies on electronic reports run via RAILS.
   d. FCOs must conduct a physical inventory audit of all empty A-file jackets and reconcile their empty A-file jacket inventory whenever there is a change in Records Managers or EJMs.
   e. BOIB will monitor compliance by randomly reviewing FCO audit reports to ensure the required semiannual audits are conducted.
   f. Resolving discrepancies
      i. If your physical count of empty A-file jackets does not match what your logs and/or Empty A-file Jacket Report indicate you should have on hand, there is a discrepancy. You may have too many folders or not enough.
      ii. First, do a recount. If you did not do the physical count in the operating units, you may wish to do so at this point.
      iii. Then if there is still a discrepancy, verify that shipments were logged correctly.
      iv. Do a physical check of the A-numbers on the logs and the A-file jackets on hand to make sure the information on the log is recorded properly.
      v. Check CIS2 to see if the A-file jackets were created.
      vi. If there is still a discrepancy the local EJM should notify the Regional/Program Records POC. The Records POC will notify BOIB at HQPCB-EM@uscis.dhs.gov with "Empty Jacket Discrepancy" in the subject line.

9. BOIB will notify program offices found not to be in compliance with audits as required by the RPM.

Chapter 12 - Deceased Applicants

1. Two primary objectives of adding a deceased code to CIS2 are to prevent fraud and to make the file eligible for retirement.

2. General rules for using the deceased code
   a. This is a function performed only by the Records Unit. Each unit will designate, and train, the records personnel allowed to add the deceased code.
   b. To limit the chances of erroneously designating people as deceased, the ability to add the code is restricted and should be added only after carefully following the steps in this chapter.
3. The COA in CIS2 when a person is deceased is "DEC."
4. Only when the proper documentation of the death is in the record can the record be updated in CIS2 screen 9316, see CIS2 user guide 4.15.11. Proper documentation includes
   a. An original death certificate issued by a governmental authority;
   b. A copy of a death certificate issued by a governmental authority; or
   c. An official notification from a state or federal agency attesting that the individual is deceased.
   d. A raised seal is not required.
5. What to do upon notification of death
   a. In order to add the deceased designation to CIS2, DHS must receive a copy of a death certificate issued by a governmental authority or official notification from a state or federal agency attesting that the individual is deceased. A raised seal is not required.
   b. If your office receives any other type of notification – such as a letter from a family member, return the notification with a letter requesting a copy of the death certificate.
      i. Make a copy of the original notification and the follow-up request.
      ii. Stamp using the action completed stamp and send to the Records Unit for interfiling.
   c. If a member of the family or other representative makes a death notification in person, ask for a copy of the death certificate. If the representative returns immigration-issued documentation, accept it. Make a notation of the circumstances. Put the action completed stamp on the documentation and send to the Records Unit for interfiling.
   d. If someone brings a death certificate with them to an office, you may make a copy and return the original. Death certificates received in the mail will not be returned unless submitted on a G-884, Request for the Return of Original Documents.
   e. Do not make an update to CIS2 until you have an official death certificate. In the interim, putting the preliminary notification material in the A-file will alert others using the file.
6. Death certificates sent to support a FOIA request
   a. When a FOIA unit receives a death certificate in support of a FOIA request, they are to make a copy of the certificate and route the original to the Records Unit.
   b. On the routing slip give the name and phone of a contact in case the Records Unit needs additional information.
7. Follow the table in Appendix B to locate the record and complete the action.

8. If the number was not provided, search CIS2 to find the A-number. Do an exhaustive search, following all the steps outlined in the search chapter, if required. If you still do not find the A-number, request a manual search request through the ORM Request website.

9. If you cannot locate an A-number,
   a. Return the death certificate to the sender and request an A-number; or
   b. If you cannot return the death certificate to the sender, you must file the death certificate in your Field Office Subject Files Correspondence for one year.
      i. At the end of the year, the office must conduct another search of the record.
      ii. If a record is located, the updating process is continued
      iii. If a record is not located, the death certificate must be shredded.

10. Updating CIS2
    a. Do not make an update to CIS2 until you have an official death certificate.
    b. The Status Change COA Screen 9316 in CIS2 is a restricted access screen. Only those with access can change the Class of Admission.
    c. Only a limited number of people should have access to this screen. If the people designated to handle deceased codes do not have access, follow the procedures in the RPM for requesting access to restricted CIS2 transactions.
    d. Have the A-file in your possession before updating CIS2. Double-check the information in the A-file, on the death certificate, and in CIS2 before changing the COA.
    e. To update the Class of Admission (COA) Screen 9316
       i. Enter the A-number of the subject.
       ii. Enter DEC in the Class of Admission Code data field.
       iii. Press ENTER. The message "Verify Data" displays.
       iv. Verify that the data entered is accurate and press ENTER to complete the system update.
       v. "The message update for this transaction has been complete" displays.

11. When updates are complete, the record must be closed and prepared for retirement. Follow the instructions for retiring A-files.
    a. When a record is in field office, it might be necessary to route the record to your local Adjudications Offices so they can check to see if the person is the principle on family-based petition and make any changes required by your local procedures.
    b. The NRC reviews these records, and if there is an open action, will forward the file to the responsible field office.
    c. When the record is returned, it is eligible for file retirement.

Chapter 13 - Classified Records

1. The USCIS Security Handbook Chapter 8 is the governing authority on matters relating to the safeguarding, management, and control of USCIS classified materials.

2. DHS contractors and employees may handle classified materials only to the extent permitted by the contract and their NSI security clearance and are responsible for handling and safeguarding any classified files assigned to them in accordance with procedures established in the USCIS Security Handbook Chapter 8.
3. For ease of reference, the Office of Security and Integrity (OSI) has also created a pamphlet, Safeguarding Classified and Sensitive Unclassified Information, that serves as a shortened digest to the governing policy.
4. See USCIS Security Handbook Chapter 8, Part C for complete information regarding the storage of classified NSI, including security container use, control procedures, and repair and maintenance.
5. All access to classified material needs to be for a legitimate business reason, or a "need-to-know." If there are any questions regarding a prospective recipient's need-to-know, the holder of the information must contact their supervisor, Records Supervisor, or local Custodian of Classified Materials before disseminating or distributing classified material.
6. Access to classified information SHALL NOT be provided to personnel without the proper NSI Security Clearance and need-to-know. Before disseminating classified information, the holder/sender of the material must confirm that the recipient possesses the required NSI clearance.
7. Confirmation of NSI clearances is provided by the OSI Personnel Security Division (PSD)- either in the form of a current access roster or via a requested records check. Contact your supervisor or OSI FSM for access roster information, or contact the PSD directly via e-mail to USCIS-OSI-PERSEC-CustomerServ@uscis.dhs.gov to check the Security Clearance status of a prospective recipient.
8. The person who first places a classified document(s) into a previously unclassified record is responsible for incorporating required classification markings and cover sheets into an A-file by:
    a. Conspicuously stamping the top and bottom of the front and back covers of the file jacket with the security classification equal to the highest classification level of any classified document contained in the file;
    b. Stapling the appropriate classification cover sheet (which can be obtained through GSA) to the front cover of the file jacket:
    c. SF-703 for Top Secret records;
    d. SF-704 Secret records; or
    e. SF-705 for Confidential records; and
    f. Attaching the appropriate classification cover sheet to the front of each classified document within the file.
    g. For more information on marking files as classified, see USCIS Security Handbook Chapter 8, Part D.

9. If a file not marked as classified is later discovered to contain classified information, the person discovering the presence of classified information is responsible for applying the required classification markings as outlined above, or for bringing the matter to the attention of an official, such as a security officer or supervisor, who will ensure that the file is properly marked.

10. Classified records must be assigned to section code "ZW" in RAILS, and an RPC within the "ZW" section must be assigned for the control and tracking of classified files.

11. Offices are also required to do the following:
    a. Establish more than one responsible party code if the volume of files containing classified information warrants; and
    b. Ensure that files containing classified information are charged only to individuals who possess the requisite security clearance.

12. Copying of classified material must be kept to an absolute minimum consistent with operational requirements and in accordance with the USCIS Security Handbook Chapter 8, Part C, Section 5.0.

13. Classified LHMs must be reviewed on the Homeland Secure Data Network (HSDN) rather than printing a hard copy.
    a. If a classified LHM is printed, it must be physically housed in a W-file. Do not place the classified LHM in a T-file.
    b. The classified W-file must be tracked in RAILS:
        i. Records Personnel is responsible for creating the W-file in RAILS.
        ii. A comment stating that the "LHM is digitally stored on HSDN" must be added in RAILS.
        iii. W-files must be stored in a ZW section code (a code reserved for classified files) and a Responsible Party Code (RPC).
    c. Classified LHM W-files must be stored in a GSA approved security container or authorized open storage area designated for classified information.
    d. The Classified LHM W-files may only contain the Classified LHM and must not contain any other documents.
    e. When the W-file containing the classified LHM is forwarded to the adjudicating office, it must be accompanied by both the required classification cover sheet (front and back) that identifies it as classified material, and the printed copy of the classified LHM received via HSDN that identifies it as part of the adjudication package.
    f. Prior to adjudication, the adjudicating office must store the W-file containing the classified information locally, in a GSA approved security container or authorized open storage area designated for classified information.
    g. If a hard copy was printed and a W-file created, the receiving office should destroy the hard copy and delete the W-file in RAILS after adjudication. A comment stating that the "LHM stored in a W-file has been destroyed" must be added in RAILS.

h. Do not save local copies of classified LHMs sent via HSDN. NBC maintains a permanent repository of LHMs on HSDN.
i. T-files containing classified LHMs may be destroyed if the classified LHM has the following notation on the top and bottom of the front page, and on the bottom of all other pages: "This LHM is digitally stored on HSDN."
j. Pending future guidance, T-files containing LHMs that are not stored in HSDN should be stored locally in a GSA approved security container or authorized open storage area designated for classified information.

Part D - Requesting, Sending, and Receiving Immigration Records

Chapter 1 - Requesting Current Records

1. Routine requests for non-retired, non-archived records must be made through RAILS, regardless of whether the record is in the same local office, a different office, or with a different agency. See RAILS transaction mapping for more information.

2. Requests are considered complete when
   a. The record is sent electronically in RAILS and prepared for mailing (if physical or hybrid record); or
   b. The record is marked In Use or Missing/Lost in RAILS and the requestor has been notified.

3. Requests for information from a record located at the NRC or an FRC:
   a. The Information Management Liaison Section (IMLS) has highly trained USCIS employees who provide quick access to and analysis of any information contained in records held at the NRC or in related automated systems. This, as well as the ability to provide copies via fax machine or email, often eliminate the need to request the record.
   b. Routine (non-emergency) requests will receive a response within 3-5 business days. For routine requests, send an email addressed to NRCINFO, NRC and include the following information:
      i. A-number;
      ii. Full name;
      iii. Date of birth;
      iv. Information or document(s) required; and
      v. Point of contact, telephone number, and fax number (if requesting fax).
   c. Priority (urgent) requests will receive a response within five hours. For priority requests call (816) 350-5560.
   d. Requests for information from records located at the FRC will receive a response within 5-7 business days.

4. For priority requests for non-retired, non-archived records located at another FCO,
   a. Non-records staff must make the request through RAILS;
   b. Records staff must contact the FCO and provide the following information:

i. A-number, receipt number, or other record indicator;
ii. Requesting FCO and RAILS RPC;
iii. Account number for the priority shipping courier service (for example, FedEx, UPS, or other), requesting office pays for shipping;
iv. Address where the record will be sent (include the local Records Office where the file will be routed through); and
v. Point of contact telephone number.

c. If the record is not going directly to the Records Unit in your FCO, the receiving FCO is responsible for coordinating in advance with the local Records Unit to ensure the record is properly tracked upon receipt.

5. For priority requests for records located at the NRC, see NRC Customer Guide Section 5.

6. To convert a routine request for a record located at the NRC to a priority request, the user must send an email request to NRC Field Processes with the following information:
   a. A-number;
   b. National emergency, national security, and/or humanitarian justification;
   c. Address of where to send the record;
   d. Account number for the courier service account (UPS);
   e. RAILS RPC; and
   f. Point of contact telephone number.

7. Non-CIS2 9506 users may submit emergency requests for records via telephone by calling the NRC Information Liaison Division (ILD) Hotline at (816)350-5560. The NRC is available 24 hours a day/7 days a week for emergency/priority information requests (except Thanksgiving and Christmas).

8. Requestors should allow eight (8) working days for routine requests and three (3) working days for priority requests before following up on a request.

9. Requests must be reconciled in RAILS using the Past Due Widget report as part of the follow-up process.

10. Requesting C-files
    a. Documents contained in C-files where the numbers are between 1 and 6,500,000 are on microfilm or on hard copy.
    b. To request a C-file, submit a manual search request through the ORM Request website.
    c. Destroy microfilm prints upon completion of review. These are unofficial prints and should not be returned to IIMD.
    d. Original records must be returned to IIMD.

11. Internal request for classified records

a. Prior to transmitting classified information, the holder of the information must contact the OSI Personnel Security Division at USCIS-OSI-PERSEC-CustomerServ@uscis.dhs.gov, or coordinate with the Classified Files Custodian or local FSM or LSO to ensure that confirmation is received before charging out a record. Do not accept verbal assurances from the requestor or verifications hand-carried by the individual.
b. Only someone with the appropriate security clearance may access and pull the record from the classified storage area.
c. The appropriately cleared staff must
    i. Ensure the file jacket is stamped with the correct classification level; and
    ii. Ensure the appropriate classification cover sheet is attached.
d. To transport the record
    i. The record may only be transported by an employee who has been issued written courier authorization from OSI. See the USCIS Security Handbook Chapter 8 Part C Section 4.0.
    ii. If the record is hand-carried to the requestor, the record must be placed in an unmarked envelope.
    iii. If the record must be transported outside of a facility, the record must be double-wrapped and packaged in accordance with the DHS Instruction 121-01-011.
    iv. If the record is transported offsite, the employee transporting the record must possess written courier authorization from OSI. Written authorization will most commonly be in the form of a "Courier Card" issued by the local OSI FSM.
e. Individuals returning classified records to the Records Unit are responsible for ensuring the records are hand-delivered to a Records staff member with the proper security clearance.

Chapter 2 - Requesting Archived or Retired Records

1. A-files of individuals born 100 or more years ago are permanently transferred to NARA and are indicated by
    a. FCO code “NMO” for NARA Archives Kansas City;
    b. FCO code “NCA” for NARA Archives San Bruno; or
    c. Transaction Indicator in CIS2 “T.”
2. NARA provides certified copies of the A-file.
3. Original A-files are provided only in rare cases and only for DHS employees.
    a. Anyone outside of DHS requesting an original A-file that resides with NARA, must submit a request through FOIA/PA.
    b. Requests for original A-files must be sent to
        i. NRC@uscis.dhs.gov if the FCO code is NMO, or
        ii. SFRREC@uscis.dhs.gov if the FCO code is NCA.
    c. Requests for original A-files must include:
        i. A-number;

ii. Alien first and last name;
iii. Name/location of the requestor (agency/FCO or sub-office code);
iv. Requestor telephone and fax numbers, and email address;
v. Request justification; and
vi. Shipping address, preference, and account information.

d. The record will be recalled under the provisions of the A-file retention schedule only if it is determined that there is a legitimate need for the original A-file.
e. The record must be FRC Returned in RAILS and transferred out to the requesting FCO. The NRC will "log" the file and monitor its use by making periodic inquiries in RAILS.
f. The requesting office will return the record in a separate package and place a routing slip on the record stating "File Must Be Returned to NARA Archives." The record must be re-retired to the old accession in RAILS and returned to NARA's custody.
   i. For NMO:
      National Records Center
      150 Space Center Loop, Suite 300
      Lee's Summit, MO 64064
   ii. For NCA:
      USCIS
      630 Sansome Street
      San Francisco, CA 94111

4. Records at the FRC belong to DHS but are in the custody of NARA.
   a. Records at the FRC must be requested in RAILS.
   b. If the record is not in RAILS, you must contact the FCO that retired the record.
   c. The retiring FCO must request the record through ARCIS and annotate the ARCIS comment block with instructions regarding where to ship the record.
   d. If the FRC cannot find the record, they will notify the requestor using the address that is on the OF11-87b Reference Request.
   e. For more information about retired records, see RPM Vol 1, Part D, Chapter 4.

5. Related T-files and interfiling must be sent directly to NARA to be interfiled.
   a. DHS may incur a charge for processing if interfiling is sent directly to the FRC.
   b. The A-number, accession number, and box number from RAILS must be included in the interfiling request.
   c. A comment must be added in RAILS stating, "Documents sent to NARA to be interfiled into A-file," and then the T-file must be deleted in RAILS.
   d. If the FCO code is NMO, send to:
      National Archives and Records Administration
      Central Plains Region
      ATTN: Elizabeth Burnes
      200 Space Center Drive
      Lee's Summit, MO 64064-1182
      (816)268-8093

e. If the FCO code is NCA, send to:
National Archives and Records Administration
National Archives at San Francisco
ATTN: Michelle Bradley
1000 Commodore Drive
San Bruno, CA 94066

Chapter 3 - Requesting Historical Records

1. USCIS has historical records that are not in the Central Index System (CIS2). The chart in Appendix C is a quick reference guide for finding and obtaining historical records. See RPM Vol 3, Part B, Chapter 7 for more details on the types of records and the information they contain.
2. Some historical records may be stored either at NARA or in an FRC.
   a. Records stored at the National Archives, are legally in the custody of NARA, who has full ownership and responsibility for the record. National Archives owned records should only be requested to satisfy an internal USCIS need.
   b. Records stored at an FRC are legally in the custody of DHS.
3. To request a record that is in the legal custody of the National Archives, offices must go through a NARA liaison.
   a. Some offices have existing liaisons (for example, Western Region FOD liaises with the San Bruno FRC).
   b. If your office does not have an existing NARA liaison or you do not know who your liaison is, you must contact the USCIS Records Officer via email at uscisrecordofficer@uscis.dhs.gov to place a request for any record that is in the legal custody of NARA.
   c. FOIA requests for records must be submitted directly to NARA.
4. Historical records housed at COW may be transferred to another FCO on loan only. The files must be returned to COW for re-filing unless they meet the conditions for consolidation.
5. Historical records not found in RAILS or CIS2 may require a manual search request through the ORM Request website if one of the following applies:
   a. The person has an A-number under 12 million or between 30 and 35 million;
   b. The A-file could have been created before December 31, 1975;
   c. The search involves non-immigrant records from before January 1938; or
   d. The search involves naturalization or citizenship records dating between 1906 and March 31, 1956.

Chapter 4 - Requesting Digitized Records from EDMS

1. If the CIS2 or RAILS status indicates digitized, the file must be viewed in EDMS.

2. In lieu of a physical paper record, you may request a CD copy of the record. See RPM Vol 4, Part B, Chapter 3 for requesting a CD copy.
3. If a certified true copy of an EDMS record is requested, follow the procedures in RPM Vol 3, Part F.
4. Requests for physical records that are stored in EDMS are evaluated by the local servicing FCO Records section. Requests must include supporting documents showing:
   a. A court order signed by a judge requesting/requiring the original physical record;
   b. Evidence the requestor is an investigator of fraudulent activity seeking the original physical record because the electronic record lacks the necessary quality (for example, fingerprint ridge detail necessary to confirm an individual's identity) and is inconclusive, as determined and documented in the final report issued by the ICE or equivalent investigative agency forensics lab; and/or
   c. The request is pursuant to an ICE declared National Security Event (NSE). Such requests will be processed in accordance with RPM Vol 6, Part B.
   d. Refer to the Physical File Release Procedures and Flow Chart documents for detailed guidance regarding the request process.
5. Agencies other than USCIS, ICE, and/or CBP should request digitized records or information through their agency point of contact or through a routine use disclosure as described by the specific Privacy Act System of Records Notice (SORN).
6. If a state or local agency wants to access records for reasons other than law enforcement or a routine use disclosure described by the specific Privacy Act SORN, they may file a FOIA request.
7. For further information, see RPM Vol 3, Part F

Chapter 5 - Searching for Records

1. Introduction
   a. Two USCIS systems track A-files: the Central Index System (CIS2) and the RAILS
   b. Record searches yield important information to support the decision process to grant or deny benefits. You should search for an A-file prior to creating a new record. Searches are initiated in response to:
      i. An outstanding record request;
      ii. The result of a record audit;
      iii. Finding A-files related to a case;
      iv. Interfiling a document; or
      v. As part of a special project.
   c. There should be only one A-file per individual. If your information suggests the person has an A-file, it is important to try multiple search techniques. The more information available to you the more search variations you should try.

d. The goal in any search is to create a query that will result in a manageable list where you can successfully distinguish your record from other records.

2. Searching for an A-file when you know the A-number
   a. Searching on an A-number is the fastest way to find a record. Older records with A-numbers may not be in any electronic system and you may need to conduct a manual search request through the ORM Request website.
   b. First check the local tracking system: RAILS.
   c. RAILS process
      i. When searching in RAILS use the Inquiry screen.
      ii. RAILS will indicate the current FCO and responsible party code of the record.
      iii. Use the "Search" box located on the dashboard.
   d. If RAILS show no master record, search in CIS2.
      i. The CIS2 FTD screen accessed by selecting PF11 from the 9504 screen is no longer be updated with record location and status information. The CIS2 FTD data froze on the date CIS2 deployed but will be available to CIS2 users to query for historical purposes. If a record is found in CIS2 it is possible that the file is a secondary record, a historical file or a retired file. Note the current FCO (Some users reported their local process for this search begins at the Display Personal Description Data Screen 9201).
      ii. Use the ID # Search/Display (ID) Screen CIS 9504 to find out if the record has been consolidated. The only consolidations CIS2 tracks are A-file consolidations.
      iii. If the current FCO is your FCO, contact the records office.
      iv. Check the FRC docket cards, if available, for FRC retirement information.
      v. If the record search results locate the record in another FCO, ensure the name and DOB of the found record match the name and DOB of your subject. If they match, request the record in CIS2 using File Transfer Request (FTR) Screen 9501.
   e. If the search on an A-number is successful, but the information in CIS2 does not match the information on the person whose record you are seeking, a transposed A-number may be the cause. Enter the record number and transpose selected portions of it as shown below:
      i. For example, you searched on A72 907 565 and the CIS2 record did not match your information. Try variations such as A72 907 556, A72 907 655, et cetera.
      ii. Users have reported the numbers most commonly transposed are the last three.
      iii. While this process sounds time consuming, it is not. System response times on an A-number search are faster than other types of searches.
   f. The primary record number for persons naturalized prior to April 1, 1956 is a C-number not an A-number. Search on a C-number by using a C rather than an A on the CIS 9504 screen. If you find the record using the C-number, request it using the C-file process.
   g. If you did not find the A-number and the number is under 12 million or between 30 and 35 million, request a manual search request through the ORM Request website.

3. Searching for an A-file without an A-number can be done in CIS2. The searches beginning at D.1 are arranged in order from highest results to lowest results. A search is not complete until you are sure no record exists. If you suspect that a record exists, you should exhaust all possible search techniques.

4. Exact name searches
   a. If you are reasonably certain of the name and the spelling of the name, the CIS2 Exact Name Search (EX) Screen 9103 provides good results. This screen will retrieve names that match exactly. If there is any variation between what you enter and the information in the system, the system will not find a match. For example, your query may be for Mary Elizabeth Smith and she is in the system as Mary Smith or Mary E. Smith you will not get results.
   b. The way CIS2 stores names can make looking for an exact match difficult. CIS2 no longer uses any punctuation or numbers in names. There are also no juniors, seniors, or numbers.

Your Source	CIS2	CIS2
O'Hara	OHARA	O_HARA
Remsky, III	Remsky	REMSKY_III
Remsky, Jr.	Remsky	REMSKY_JR

   c. CIS2 treats spaces as characters. If someone hits the space bar after entering the name, CIS2 records this as a character. To CIS2 the blank space is a character that is just as important as any letter. Since the screen does not show the difference between a blank space and nothing, you cannot tell the character space is present.
   d. If you put together the two situations, no punctuation and invisible characters for spaces, this increases the possible ways a person's name might appear in CIS2.
   e. This has the most consequences when searching for an exact match. For example, you might be searching for a Margaret O'Malley. CIS2 could have any of the following entries for this person (a "%20" represents a blank space).

First Name	Last Name
MARGARET	O_MALLEY
MARGARET	OMALLEY
MARGARET_	O_MALLEY
MARGARET_	OMALLEY
MARGARET_	O_MALLEY_
MARGARET	OMALLEY_

   f. When doing an exact name search, or looking for a person who might or might not have spaces in their name, you should try a few variations.

g. Exact name searches are fast, but if you do not get results using this search, do not assume the person is not in CIS2.
h. If your search results are unsuccessful, select the PF9 (or your system's equivalent) key and this will take you to the Sounds-Like Name Search (SL) Screen 9102.
i. Information, not in CIS2, from legal source documents should be used to update CIS2. Only authorized personnel can update CIS2

5. Sounds-like searches
   a. Queries made using the CIS2 Sounds-Like Name Search (SL) Screen 9102 find all names with similar spellings. It is the most commonly used searching screen in CIS2 because it generally gives the best results.
   b. You may also want to check the spreadsheet that gives variations in spelling for common names.
   c. Sometimes you will get lists of names that do not seem related. For example, a Sounds-Like search on Smith will also find Schmid and Sonato.
   d. This is because Sounds-Like is based on SOUNDEX codes. SOUNDEX assigns a four-character code to all names using the initial letter of the name plus three numbers according to a set formula. Query results will contain names with matching codes.
   e. While this might seem confusing, it is very helpful. Some names in the CIS2 database are translated from other languages and other alphabets. Therefore, the spelling in English is not always consistent. Sounds-Like also allows for this and possible data entry errors.
   f. This search can retrieve thousands of names. The screen displays 12 names at a time. You can follow system prompts to back out of the screen and try to narrow the search with more information to retrieve more concise results.
   g. If the information you add does not match what is in CIS2, the person could be in the system, but not on your list. For example, suppose your search was for Mary Smith born on December 12, 1964, in Mexico (Country of Birth) and a citizen of Guatemala (Country of Citizenship). If the system mistakenly has Mexico as both the COB and the COC, a search on the correct information will not find her.
   h. If you have entered just the name and DOB, CIS2 will automatically jump to the Soundex with DOB Name Search Screen 9106. You don't have to re-key the information, but your search results will show on the 9106 screen. Section G.4 provides information on searching on dates in CIS2.
   i. If your search results are unsuccessful and you have an alias, select PF9 (or your system's equivalent) from the Sounds-Like screen. This will take you to AKA (Alias) Name Search (AKA) Screen 9104.
   j. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated. Only authorized personnel can update CIS2.

6. Alias (AKA) searches
   a. Use CIS2 AKA (Alias) Name Search (AKA) Screen 9104 to search for a person using alternate names. The name you have could be an alias.

b. This screen is especially useful for cases where people have Americanized their name, married, made legal name changes, or have aliases.
c. Selecting PF9 (or your system's equivalent) while you are on this screen will return you to Sounds-Like Name Search (SL) Screen 9102.
d. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated. Only authorized personnel can update CIS2.

7. Sounds-like name with date of birth
   a. Be careful when entering dates into CIS2 screens. In CIS2, you enter digits for the month (MM), day (DD), and year (YYYY). For example, December 5, 1970 is (12)(05)(1970). CIS2 accepts 00 for month and 00 for day.
      i. Immigration forms are not always consistent in how they ask for dates. Sometimes they ask for the day first. If a search is not successful and the date is one where a transposition of day and month is not obvious, try transposing the two.
      ii. It is the custom in many countries to write the date DDMMYYYY. If your date is from a foreign document, be aware of the date format.
   b. If there is some uncertainty about the exact date of the person's birth or an exact DOB does not give retrieve a record for someone you are fairly certain has a CIS2 record, use Soundex with DOB Name Search Screen 9106
   c. You need the last name, first name, and some form or variation of DOB to use this screen.
   d. Some variations of DOB are:
      i. Exact DOB
      ii. DOB Year Range: You enter the four digits for the year and then a number from 0 to 9. The 0 to 9 defines the range of years you want to search. For example, if you enter 19737, CIS2 will search for persons with the name you gave and a year of birth between 1966 and 1980. If you enter 19581, CIS2 will search for birth years between 1957 and 1959.
      iii. DOB Month Range: You enter the four-digit year, two-digit month, and a number from 0 to 12. The 0 to 12 defines the number of months searched around the given date. For example, if you enter 19480103, CIS2 will search for people with the name you gave and a date of birth between October 1, 1947 and April 30, 1948.
      iv. DOB Day Range: You enter the four-digit year, two-digit month, two-digit day, and a number between 0 and 31. The 0 to 31 defines the number of days searched around the date given. For example, if you enter 1952120730, CIS2 will search for people with the name you gave and a date of birth between November 7, 1952 and January 6, 1953.
   e. You can narrow the search by specifying the country of birth.
      i. You may want to check tables for the country code. They are not always what you would expect. To check the tables, press Clear All, type in Table, select PF7 (or your system's equivalent) to list the tables, and select the appropriate table off the scrolling menu.

ii. For example, the code for Cambodia is KAMPU not CAMBO. Since Australia and Austria have the same first five letters, CIS2 refers to them by the last five letters – STRIA and RALIA. Most of the country codes have five characters, but some like England (UK) and the Dominican Republic (DR) do not.

f. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated. Only authorized personnel can update CIS2.

8. Searching by identity numbers
   a. CIS2 ID Number Search (ID) Screen CIS 9504is not just for searching by A-number. The following are identification numbers you can search on:
      i. A-number: Search by A-number
      ii. AA: Certificate of Citizenship Number
      iii. C: Naturalization Certificate Number. Normally older records, C-files located in the history.
      iv. DA: Derivative Citizenship Number
   b. The following numbers are not always in CIS2, however, these searches are quick and should be tried:
      i. DL: Driver's License Number;
      ii. FB: The FBI Number is on fingerprint cards (FD-248 and FD-249). The red fingerprint cards are on criminals. On these, the number stays the same. On the blue fingerprint cards, FD-258, the numbers are temporary;
      iii. I-94: Admission Number. This is the number of the current I-94. You must have all 13 numbers of the I-94 in order to search using the I-94 number;
      iv. PP: Passport Number;
      v. SS: Social Security Number; or
      vi. TD: Travel Document Number. This number comes from advanced paroles – a document used for reentry.
   c. Screen CIS 9504 displays more personal data than other CIS2 screens. It shows if:
      i. The record was consolidated and the primary record; and if
      ii. A card was produced.
   d. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated. Only authorized personnel can update CIS2.

9. Legalization adjustment processing screen (LAPS)
   a. Legalization numbers are primarily in the 90 to 93 million series. If you are searching for someone whom you know (or suspect) has filed a legalization application, this CIS2 screen helps narrow your search.
   b. Use LAPS (Exact) Name Search (LAPS) Screen 9105.
   c. You must have a last name, first name, exact DOB, and COB for this search.
   d. CIS2 will search only 90 million numbers initially. If it doesn't find a match, it will do a name search of the rest of the numbers. People who adjusted their status, were given a 70 million number as part of the adjustment process.

e. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated. Only authorized personnel can update CIS2.

10. Updating the information in CIS2
    a. Only authorized personnel can update CIS2. If your information is from a legal source document and that information is not in CIS2, CIS2 should be updated.
    b. Use Maintenance of Personal Description Data (MPER) Screen 9411 (a restricted access screen) to update everything except the COA, the FCO, aliases, and Naturalization information.
    c. If you have the record and the FCO is incorrect, contact the FCO listed and ask them to check their RAILS: If they have the same record and both have the same prefix, send both files for reconciliation to the NRC. Only send files that have fully closed and adjudicated applications and actions.
    d. The NRC address is: Department of Homeland Security 150 Space Center Loop Lee's Summit, Missouri 64064
    e. If they do not have the record, use File Transfer Maintenance (FTM) (a restricted access screen) to correct the FCO. Do not use this screen to update an FCO other than your office. Then be sure to update your local RAILS with the correct file location.
    f. To update the COA, use Class of Admission (COA) Screen 9316 (a restricted access screen).
    g. To update the aliases use Add AKA (Alias) Name (AAKA) Screen 9303.
    h. To update the Naturalization information use NATZ Stub (NS) Screen 9311.

11. When you don't find a record in CIS2/manual searches
    a. When DHS Offices are not able to find A-file information on an individual in CIS2 and they are relatively certain that DHS has immigration records on the individual, the office may request a manual search request through the ORM Request website if the applicant was born and entered the U.S. before December 31, 1975.
    b. For an overview of the web site and step-by-step instructions on how to create an account and how to submit requests, refer to the User Guide for the ORM Request website.

Chapter 6 - Sending and Returning Records

1. All record movements must be recorded in RAILS using the correct transaction codes. See RAILS transaction mapping for more information.
2. Records must be returned to the Records Unit once action has been completed on the file.
3. When sending physical immigration records to another office, each box or package must be manifested.
    a. The manifest must indicate, at a minimum, the file numbers in the box or package, the sending and receiving office code, the box or package number (for example, "1 of 5"), and the date.
    b. A hard copy of the manifest must be placed in each box or package and a hard copy or electronic copy kept by the sending office for file accountability.

c. Once the shipment has been received and accounted for at the receiving office, the manifests can be destroyed. Manifests containing A-numbers must be handled as Sensitive PII.
d. If a box or package is lost during transport, a copy of the manifest indicating which files are lost must be included with the SIR.

4. Each box or package to be shipped must
   a. Be assembled in bulk, individual files will not be accepted;
   b. Not be filled tightly in order to avoid damage in transit;
   c. Be double-sealed with filament tape with fiber; and
   d. Not have tape over box handles (hand holes).

5. When sending records to NRC or HBG for retirement, different file/form types must not be mixed as they have different retention schedules. See USCIS retention schedules.

6. Closed physical and hybrid Receipt files must be sent to the HBG.
   a. For a list of acceptable physical Receipt files to send to the HBG see Appendix D.
   b. Follow the procedures for storing and mailing files to the HBG in the NRC Customer Service Guide.
   c. Because boxes may remain in loading docks for an extended period of time, local procedures must define controls for tracking each record in a particular shipment (and box for bulk shipments) to enable retrieval in an emergency or within 12 days of receipt.

7. Closed physical and hybrid A-files must be sent to the NRC.
   a. For a list of physical and hybrid A-files to send to the NRC see Appendix E.
   b. Follow the procedures in the NRC Customer Service Guide.

8. Records retrieved from the San Bruno FRC must be returned to the San Bruno FRC via the San Francisco Field Office. These files will have a stamp on the jacket from AGA, HHW, REN, or SFR.

9. Additional procedures and regulations regarding transmission of classified records are maintained in the USCIS Security Handbook Chapter 8, Part C, Section 4.0.

Chapter 7 - Responding to Requests for Records

1. The local Records Unit is responsible for processing requests for physical and hybrid records located within their FCO. Responsibilities include:
   a. Generating pull tickets daily;
   b. Sending pull tickets and File Request Status Inquiry Form to the person or unit holding the record;
   c. Sending appropriate reminder emails and updating the File Transfer Indicator Code in CIS2 when the responsible party does not respond;
   d. Retrieving records from file rooms;
   e. Attaching pull tickets to the files;
   f. Preparing and mailing records;

g. Completing special searches if the record cannot be found;
h. Generating and reconciling RAILS/SMART reports.
i. Retaining records of emails for one year and then deleting.

2. Individuals in operating units are responsible for:
   a. Responding promptly to requests for records in their RPC;
   b. Providing a valid reason to place a requested record In Use if it cannot be released;
   c. Working with requestors to provide either the record or the information needed to make an accurate and timely decision; and
   d. Reporting lost, destroyed, or damaged records to the Records Unit.
3. Unit supervisors and managers in operating units are responsible for:
   a. Ensuring individuals respond to record requests according to the required guidelines; and
   b. Following-up on late responses.
4. Requests for records must be processed through RAILS.
   a. All parts of a multi-part record must be sent to the requestor;
   b. Pull tickets generate at 14-day intervals and continue to generate through the 6th and final pull ticket, when the request is complete or canceled.
5. Requests for physical and hybrid records from inside your FCO must include the File Request Status Inquiry Form.
6. Requests from outside your FCO:
   a. Operating Unit staff should forward the request to their Records Unit;
   b. Records Unit staff must follow the directions in either RPM Vol 3, Part D, Chapter 1 or RPM Vol 3, Part F as appropriate.
7. Requests for a physical record located in the FRC, the Records Unit must
   a. Request the record in RAILS;
   b. Take the record out of accession and return it to active status by using the FRC Return Transaction;
   c. Attach the pull ticket to the record and forward the to the requestor.
8. FOIA/PA requests must be responded to within 20 working days. See 5 U.S.C. 552.
9. Responding to routine requests:
   a. Operating units have 24 hours from receipt of the request to respond.
   b. Records units have 72 hours from receipt of the request to complete the request.
10. Responding to priority requests:
    a. Operating units have four (4) hours from receipt of the request to respond.
    b. Records units have 24 hours from receipt of the request to complete the request.
11. Responding to requests for classified records must follow additional guidance; see USCIS Security Handbook Chapter 8.

12. When more than one office needs a record, use the following priority list to determine where to send the record.
    a. Law enforcement actions including special projects like the Joint Terrorism Task Force (JTTF);
    b. Requestor has the subject of the record in custody;
    c. Court cases;
    d. Revocations;
    e. Naturalization processing;
    f. Nicaraguan Adjustment and Central American Relief Act (NACARA) requests;
    g. Congressional requests; then
    h. Freedom of Information Act.
    i. Records containing the following applications/petitions are not governed by the above priority list:
        i. Form I-360, Petition for Amerasian, Widow(er), or Special Immigrant, Form I-914, Application for T Nonimmigrant Status, and Form I-918, Petition for U Nonimmigrant Status. Records containing these petitions are identified in CIS2 with COA code 384, and all inquiries regarding these records must be sent to the Vermont Service Center.
        ii. Form I-821D, Consideration of Deferred Action for Childhood Arrivals, inquiries should be sent to Nebraska Service Center DACA team.
    j. If there is still a question of priority after reviewing this list, the offices requesting the record must work together to determine which office has the priority.

Chapter 8 - Responding to Requests If You Work in an Operating Unit

1. If you receive a pull ticket or File Request Status Inquiry Form for a record that you have, you must respond to the request within 24 hours by:
    a. "Send"ing the file in RAILS and delivering the record and the File Request Status Inquiry Form to the Records Unit; or
    b. Placing the file "In Use", marking the number of days desired, and entering the reason for holding the file.
    c. Until the record is released, the Records Unit will send follow-up requests every 14 days.
    d. If you do not respond to record requests, the Records Unit will follow-up via email to the unit supervisor as necessary.
    e. The person requesting the record may need to contact you in order to get information from the record if you cannot release the record.
    NOTE: In RAILS, the office holding the record cannot cancel the request. If required, the requesting office must perform the cancellation.
2. Summary of actions for operating unit staff:

The Request is From	You Can Release the File	You Still Need the File
A person with the subject of the A-file in custody	Work with your local Records Unit to send the file	You must release the file
Another Person in Your Operating Unit	RAILS "Receive" transaction	Place record In Use in RAILS
Another Person in Your FCO	sender RAILS "Send" function recipient RAILS "Receive" function	Place record In Use in RAILS
A Pull Ticket	Return the file to Records. The Records Unit will handle the rest of the transaction.	Use the File Request Status Inquiry Form to indicate why you still need the file. Return immediately to the Records Unit.
An individual not in your FCO	All requests should come through RAILS.	Place record In Use in RAILS
Someone not from one of the Immigration Bureaus	Refer them to your local Records Unit	Not applicable

Chapter 9 - Receiving Records
All records must be received in RAILS in a timely manner.

Part E - Correspondence and Original Documentation

Chapter 1 - General documentation guidance

1. Immigration files are USCIS records and only USCIS, CBP, or ICE personnel are permitted to interfile documents into these records. Other agencies should send documents that they would like to place into an immigration file to USCIS Records for final determination.
2. Extraneous and/or non-related materials must not be placed in immigration records (for example, screen prints) unless otherwise required by law, regulation, policy, or other appropriate authority.
3. Multiple copies of the same document must not be placed in the record, unless an authority requiring placement of the copy in the record exists. If the "copy" is not an exact duplicate, for example notes are written on the "copy" but not the original, then both documents must be included.

4. Original documents must not be placed into the immigration record, unless the document is stolen, counterfeit, altered, or presented by an imposter, or is otherwise necessary for an investigation, removal action, or enforcement action. See RPM Vol 3, Part E, Chapter 7. Photocopies of these documents must be placed in the record to support the adjudicative process and in accordance with adjudicative directives, and only the photocopy receives any stamps, such as Action Completed. The original document must be returned to the submitter when no longer required by DHS. (See 8 CFR 103.2).
   a. Adoption decrees;
   b. Birth certificates;
   c. Marriage licenses;
   d. Divorce decrees;
   e. Death certificates;
   f. Foreign passports; and
   g. Naturalization certificates.
5. Any non-standard paper mediums, such as sticky notes, must be placed in the corresponding physical file on standard 8 ½" by 11" paper. Notes and sticky notes: Adjudicators are often required to take notes regarding a case. However, they should avoid jotting down notes, comments, or opinions on the documents in the A-file unless the placement of such notes is necessary to preserve their context. Additionally, care should be taken before adding sticky notes to an A-file. Individual sticky notes often fall out of files or are misplaced and information is lost. Offices should eliminate the use of sticky notes or any other such temporary non-standard textual material. Instead, adjudicators are encouraged to use official memorandum to file, adjudication logs (work note logs), or other means to record work product on standard size paper.
6. Emails should be included in the immigration record only when they are relevant to the record and material to the adjudicative process. Once an email is added, it becomes a part of the permanent record and may be subject to disclosure, even if it contains information comments or statements that are not relevant to the record or the particular adjudication being undertaken.
7. Routing slips, staples and paper clips: Care should be taken when adding routing slips, staples and paper clips to the A-file. Although adjudicators must abide by all applicable regulations and policy, excessive addition of these items to the A-file increases the time and cost associated with scanning A-Files for digitization.
8. Temporary records: Do not add any items that are not permanent.

Chapter 2 - Interfiling

1. Interfiling is loose material or a set of related documents awaiting placement into A-files, Receipt files, Alpha files, and Subject files. Note that adding information to the right side of a record does not necessarily protect it from being subject to release through FOIA, this includes sticky notes and adjudication comments.

2. Interfiling must be processed within five (5) working days, sooner if required by local procedures, or 15 days for the NRC; and is identified by one of the following:
   a. Mail Routing Guide: local aid for the most common types of mail.
   b. Interfiling Cover Sheet: cover sheet for routing non-action interfiling.
   c. Action Completed Stamp: notifies the Records Unit that an officer has seen the document, taken the appropriate action, and is routing it to be interfiled.
   d. Non-action material is record material that requires no further action and can be interfiled immediately.
   e. If the material was sent to an operating unit other than the one specified in the mail routing guide or another FCO for interfiling, it must have an interfiling cover sheet.
      i. Use a separate cover sheet for each type of document.
      ii. Ensure that the cover sheet indicates that all action is completed.
3. Request for Evidence (RFE) materials related to applications, petitions, and requests must be interfiled.
   a. If the record is physical, then the material is filed in the physical record and forwarded to the local office for action.
   b. If the record is electronic, then the material is scanned into ELIS; verified to ensure that the image is legible and meets NARA standards; and maintained in accordance with the ELIS vs Legacy System Paper Handling Chart. For information on handling ELIS-related material shipped to HBG, see the Interim Guidance Regarding the Proper Handling of USCIS ELIS Related Material.
   c. If the record is hybrid, RFE materials must be scanned and added to one of the three NARA approved electronic repositories (ELIS, STACKS, or EDMS) where the rest of the ROP for that application or petition exists. This must be done in accordance with each system's quality control/quality assurance and records handling procedures.
4. When handling original documents, including sending to another office for interfiling:
   a. Do not stamp, write on, or hole punch the document; and
   b. Clearly identify the associated A-number or receipt number.
5. Timeliness Standards
   a. The preferred method is to routinely date-stamp all interfiling material as it is received into the records unit. If interfiling leaves the records unit for further action, re-stamp it when it is returned. Exception: original documents must not be date stamped.
6. Screening
   a. Ideally, there is no action material in the interfiling. If you find some, return it to the mailroom for appropriate routing. On the routing slip indicate:
      i. Action Material PLEASE ROUTE APPROPRIATELY;
      ii. Date sent;
      iii. Originating office;
      iv. Printed name of person forwarding the action;
      v. Contact phone number; and

vi. A-number (if appropriate).

b. Route death certificates to the person assigned to update CIS2 with the deceased code.

c. The most common error is not reading documents, especially correspondence. Some clerks will simply search for an A-number and assume the document should go directly in the file. Examples of some mistakes are:
   i. Instead of sending evidence for a case to the investigator to whom it was addressed, a records technician routed the evidence to the file.
   ii. A letter from a naturalization applicant asking to have their appointment rescheduled is not forwarded to the adjudication section, but simply placed in the file folder.
   iii. Rather than routing a letter from an individual asking for the status of their case to someone who can answer it, the letter is filed without taking action.

d. Sort documents into two groups:
   i. Non-record: set aside for destruction.
   ii. Interfiling: sort the remaining documents by the correct file series.

e. Choose the appropriate file series.

7. Use the following table to determine the correct file series:

File Series	Description
Receipt files	**Kept in Service Centers or Harrisonburg** • On the list of Alien-related files other than A-files • Relates to an individual • Related to benefits or petitions for non-immigrants OR • Immigrant related documents with short retention periods • Has receipt file number
Alpha files	**Kept in the Districts** • On the list of Alien-related files other than A-files • Relates to an individual • Related to benefits or petitions for non-immigrants OR • Immigrant related documents with short retention periods.
A-files	• Relates to an individual • Related to granting of immigrant or naturalization benefits OR • Related to enforcement of immigration law • Not on the list of Alien-related files other than A-files
Subject files	**One of the following types of information:** • Administrative matters • Personnel records • Internal memorandums • Congressional correspondence • Routine correspondence including inquiries from aliens on the status of their case • Other matters addressed in the Uniform Subject Filing System Guide

8. When processing interfiling, you may want to use the sample routing slip to record your actions.

9. Follow these steps when interfiling A-file material. Please be advised that this is a decision. You won't go through every step for every document. The results of each decision lead you to the next appropriate step.
   a. Be sure the documents have been screened.
   b. Check the document for a valid A-number.
      i. Valid A-number, go to step c.
      ii. No valid A-number, search for the A-number in CIS2 using biographical information from the interfiling. If there is not sufficient biographical information to locate the person in CIS2, treat it as a non-record.

- If found, mark the A-number on the document. Check the FCO. If the file is in your FCO, go to step c, if the file is not in your FCO, mark the FCO on a routing slip or cover sheet and go to step f.
- If not found and the document triggers an A-file creation, create a new A-file.
- If not found and the document does not trigger an A-file creation, give it to the person designated by your supervisor. This should be a person skilled in CIS2 searching. If this person also cannot match the document to an existing A-file, destroy it as a non-record.

c. Search RAILS for the file location.
   i. If found in RAILS:
      - Mark the location on a routing slip or cover sheet. Sort the interfiling in location order;
      - Ensure documents are filed the day you mark them. Otherwise, it is possible someone will move the file and you will have to start the process of locating the file all over again; and
      - Go to step e unless the file is in the FRC, then go to step f.
   ii. If not found in RAILS:
      - Check CIS2. The A-number may be incorrect or the A-file may be in another FCO.
      - Go to step d.

d. Check CIS2 for the A-number (Skip this step if you found the file in RAILS).
   i. If found in CIS2:
      - If CIS2 shows the file is in another FCO, mark the FCO on the routing slip or cover sheet and go to step f.
      - If the file number was incorrect and the file is in your FCO, correct the A-number and go back to step c.
      - If the file number is correct and CIS2 shows the file is in your FCO, but RAILS does not, follow the procedures for special searches to try and locate the file. If you still cannot find it, declare the file lost.
      - If the file is lost, begin the Lost/Missing file process as appropriate. If documents require tracking before 60-day Sub-file creation waiting period is met, make a T-file for the interfiling material.
   ii. If not found in CIS2:
      - If the document triggers an A-file creation, create a new A-file.
      - If the document does not trigger an A-file creation, give it to the person designated by your supervisor. This should be a person skilled in CIS2 searching. If this person also cannot match the document to an existing A-file, destroy it as a non-record.

e. Put the document in the file.
   i. Before putting the document in a file, ensure the information – particularly name and A-number -- on the document matches the information in the file.

ii. If the information on the document does not match the information in the file,
- The document is a package that is an ROP, attach to the left side of the file with the newest ROP on top. Be sure each ROP has a cover sheet, M-175. You may have to add a cover sheet to the top ROP in the folder.
- The package is not an ROP or is a loose document, fasten to the right side with the newest information on top.

f. What to do if the file is in another FCO or the FRC.
   i. The file is at the NRC, FRC, WCF, LSC, or HBG, see the specialized directions for the NRC, FRC, LSC, or the HBG
   ii. The file is at an FCO other than those listed above, forward the document to the FCO with the file. Include a routing or cover sheet indicating the document is for interfiling. Be sure the document has the A-number clearly marked. Do not use expedited mailing for interfiling unless you have specific approval.

10. Before inserting a document into the file
    a. Before putting a document in the file, make sure it relates to the individual in the file. Check to be sure the name and A-number match the top documents in the file.
    b. If the document does not match the contents of the file and it appears that the wrong A-number is on the document, make a note on the document. Go to step 4 in the interfiling process.
    c. If it looks like there is material from more than one person in the A-file or you have already determined the information in CIS2 matches the biographical information on the individual in the interfiling, pull the file.
       i. Some type of problem has occurred. You will need to examine the contents of the folder and compare them to information in CIS2 and possibly other systems such as CLAIMS and DACS.
       ii. See your supervisor if you need assistance or guidance.

11. Sending interfiling to another FCO
    a. When sending interfiling to another FCO, at a minimum batch interfiling and use a routing sheet that indicates that this is interfiling and which office sent it.
    b. If you batch interfiling for more than one person, do not staple everything together.
    c. You may use the sample routing slip and group documents by A-number. Make sure that any action documents have been annotated to show that the action is complete.
    d. When sending original documents to another office for interfiling, the A-number associated with the document must be clearly identified. Documents that do not clearly indicate an associated A-number will be returned to the sending office.

12. If the file is in the FRC
    a. If your FCO did not retire the A-file, send the document to the FCO that retired it.

b. The National Records Center (NRC) is not the same as a Federal Records Center (FRC). The NRC does not have access to the information required to forward interfiling to the appropriate FRC. If your office sends FRC interfiling to the NRC, the NRC will send it back to your office.
c. If your FCO retired the file, send the interfiling to the FRC that has the file. Use a routing sheet that indicates that the documents are interfiling and provide the transfer number, box number, records center location number, and correct file designation. If you have a number of pieces to go to the FRC, arrange them in accession number, box number, and location order. The FRC will return material that is not properly arranged.

13. Interfiling for the NRC, HBG, Lee's Summit MO FRC, and the Law Enforcement Support Center must not contain any incomplete or unfulfilled requests or actions; the outside of the envelope or box must say "Interfiling;" and it must not be shipped via expedited mail.

14. For address, instructions, and information on authorized interfiling for the NRC, see the NRC Customer Guide.
    a. HBG interfiling address:
    HBG File Storage Facility
    1344 Pleasants Drive
    Harrisonburg, VA 22801
    b. Lee's Summit MO FRC interfiling address:
    Lee's Summit Federal Records Center
    200 Space Center Drive
    Lee's Summit, MO 64064-1182
    c. Law Enforcement Support Center interfiling address:
    Law Enforcement Support Center
    188 Harvest Lane
    Williston, VT 05495
    d. When sending interfiling to NRC, verify that the file is indeed at that office. If the file is in transit, retain the interfiling until the file is received at that location. If the NRC receives interfiling for an alien file that is in transit, they will return it to your office.
    e. Be sure the information is not action material. Action material will be returned to the sending office.
    f. The NRC and HBG cannot:
        i. Respond to status inquiries from the public;
        ii. Respond to information requests from the public;
        iii. Update address changes in the appropriate systems;
        iv. Receive and process money;
        v. Adjudicate applications and petitions; or
        vi. Interfile material into files at the FRC. If the file is located at the FRC, follow the directions for sending interfiling to the FRC.
    g. See the Subject Filing Guide (in INSERTS) for addresses of other Federal Records Center.

15. Interfiling into Alpha files: if the table above says to file in an Alpha file, follow the directions in the chapter on Alpha filing.

16. Interfiling material into Receipt files
    a. Receipt Files are kept at Service Centers. HBG (Harrisonburg) keeps closed Receipt files.
    b. Documents for Receipt files generally have a receipt number on them. The receipt number is:
        i. Three letter prefix for the Service Center:
            - LIN. Nebraska Service Center (NSC)
            - EAC or ESC Vermont Service Center (ESC)
            - WAC or WSC. California Service Center (WSC)
            - SRC or SSC. Texas Service Center (SSC)
            - MSC Missouri Service Center (NBC)
            - YSC Potomac Service Center (PSC)
        ii. Two digits signifying the year.
        iii. Three digits signifying the Julian date.
        iv. Five digits indicating the sequence.
    c. An example of a receipt number is LIN-98-123-58970.
    d. To interfile into a Receipt file: find the Receipt file number in RAILS. If the file is located in your service center, file the document. If the file is in Harrisonburg, send it there.
    e. If the receipt file is not in your Service Center, check CLAIMS to see which office has the file. Send the document to that Service Center.
    f. Forward interfiling material to HBG if an RAILS inquiry indicates the file is located at HBG. Only request Receipt Files when an action is required. Prior to forwarding ensure that the receipt number is readable on the interfiling.

17. Authorized items that you may send in a T-file to the NRC:
    a. Closed Receipt file applications consolidated into T-files.
    b. Interfiling relating to a digitized A-file completed by the NRC addressed to SODA scanning.
        i. Any interfiling that needs to be attached to a digitized file needs to be sent to NRC as a T-file, not intermingled with A-files. It must be clearly marked as RDF Interfiling to the NRC.
        ii. Any RAILS updates must be made current (especially NATZ information) prior to T-file being sent. Do not expect receipt files to be electronically combined in RAILS after the receipt has been physically combined with the A-file and the A-file has been digitized.
        iii. Send RDF interfiling to NRC, 150 Space Center Loop, Lee's Summit, MO 64064.
    c. Deportation documentation and ICE enforcement actions, including foreign passports; and

d. OCC court cases.

18. All other documents must be sent as interfiling if the NRC is the FCO of the related A-file.
19. For related t-files and interfiling for records at NARA, see RPM Vol 3, Part D, Chapter 2.
20. Interfiling for digitized EDMS files is managed by the NRC. Refer to the NRC Customer Service Guide for instructions on processing.
    a. If a file is digitized, CIS2 will identify the File Control Office (FCO) as "DIG".
    b. Interfiling for digitized files retired and located at the FRC must be sent to the NRC not to the FRC for drop filing.
21. Upon completion of processing Form I-821, Application for Temporary Protected Status; the file should be sent to the NRC.
22. Interfiling for files stored at NARA, must be sent directly to NARA (not the FRC) so that DHS does not incur any charges for processing. The A-number, the accession number, and box number from RAILS must be indicated on the interfiling.

Chapter 3 - Action Material

1. Purpose and applicability
    a. Purpose: this section provides procedures to ensure that all actions are completed before documents are filed.
    b. Applicability: this section applies to all DHS employees and contractors responsible for taking an official action on DHS action materials.
    c. History
    d. The Office of Internal Audit completed a study on unfiled material. The results were that:
        i. Not all actions were completed;
        ii. It was impossible to determine if an action had been completed on many of the documents;
        iii. Some documents did not need to be placed in the file or retained;
        iv. Some documents needed to be filed, but not in an A-file; and
        v. Some documents needed to be in the A-file.
        vi. DHS initiated swift corrective action. These actions will ensure that:
            - Important documents will not be misplaced;
            - Fewer customers will come to DHS offices seeking information or assistance; and
            - Benefit and enforcement decisions will be made on complete information.
2. Action material is a broad term that includes any document that requires an action or decision by a DHS employee or contractor.
    a. The most common types of action documents are:
    b. Requests from customers asking for information or an action (that is, such as the status, expedited service or withdrawal of application);

c. Documents that require a system update (for example, Form I-407, Record of Abandonment of Lawful Permanent Resident Status);
d. Responses to DHS requests for evidence;
e. Motion to reopen case;
f. Undelivered mail;
g. Cash, checks, and money orders;
h. Unadjudicated applications or petitions; and
i. Death Certificates.

3. The action official is the person responsible for making a decision and/or completing the action on the action material. This can include an adjudicative decision, updating a system, or responding to a customer.
   a. When you receive action material, take the appropriate action based on the type of document.
   b. Before you file these documents, ensure that the Action Completed Stamp is present.
   c. Route stamped material for filing immediately.
   d. Stamp the document when:
   e. Action has been completed;
      i. No action is needed; and
      ii. System will not allow the update (that is, address change).

4. When routing action material to another FCO, you must attach an Action Material Routing Slip that indicates:
   a. Action material;
   b. To (if known);
   c. Date sent;
   d. Originating office;
   e. Printed name of person forwarding the action;
   f. Contact phone number;
   g. A-number (if appropriate); and
   h. A summary of any actions taken.

5. Documentation received from another FCO without an Action Completed Stamp or Action Material Routing Slip will be returned to the contact person for that FCO.

6. Before action material is routed or filed (with the exception of death certificates), it must be stamped or annotated showing the action is complete.

7. An action completed stamp or annotation must show the initials and FCO/Unit of the person who completed the action and the date the action was completed. The following documents do not need the Action Completed Stamp
   a. Fingerprint cards;
   b. I-89 forms;
   c. Identity History Summary (formerly known as RAP sheet);

d. Visa packets;
e. Death Certificates;
f. Applications/Petitions (with action taken annotated or attached); and
g. Original documents should never be stamped with the Action Completed Stamp.
h. See the chapter on Changes of Address for specific instructions on when to stamp changes of address.
i. Often the Records Unit is not responsible for taking the needed action. It is, however, the responsibility of the Records Unit to verify that the Action Completed Stamp is present.

8. Action completed stamp
   a. Following is an example of the Action Completed Stamp:

ACTION COMPLETED	APPROVED FOR FILING
Initials: FCO/Unit:	Date:

   b. Offices may add additional information to the stamp if desired. You may use this sample specification to requisition stamps.
   c. Stamp or annotate the document in the lower right-hand corner when possible.
   d. The Action Completed Stamp is not required if you file the document after taking action. Use the stamp when you complete an action on a piece of loose material and then send it to someone else to file.
   e. Everything being routed to a file must have this stamp (with the exception of items listed in section J). The mail routing guide must indicate where the document is routed.

9. When more than one person takes action on a document
   a. Some documents require action by more than one person. The person who takes the final action will stamp the document.
   b. To ensure that action material is properly routed to the next person, use a routing slip labeled Action Material. Local offices may develop a routing slip or modify the sample provided.

10. If your office receives a document from another FCO without an Action Completed Stamp or Action Material Routing Slip, the assumption will be that no action has yet been taken.

11. Death Certificates
   a. Death Certificates must be routed to the person responsible for updating CIS2 with the deceased code.
   b. Death certificates are A-file material.
   c. Death certificates do not need an Action Completed Stamp.

12. PAS reporting requirements
   a. PAS does not report Action Material. After all action is completed, the material becomes interfiling. Report Interfiling on line 700.10 of the G-22. Be sure to refer to the instructions for the PAS when completing your report.

b. For Action Material/Interfiling, count the time and the total number of pieces handled.

Chapter 4 - Change of Address and Returned Mail

1. 8 CFR 265 requires that all aliens who are
   a. 14 years of age or older;
   b. Intending to stay in the U.S. for more than thirty days; and
   c. Not in A, G, or NATO nonimmigrant status

   submit any change of address to USCIS within ten (10) business days. See AR-11, Alien's Change of Address Card for instructions on how and where to update an address, including special circumstances.
2. The USCIS Contact Centers accept some address changes over the phone, but they are also asked to submit an AR-11.
3. If your local office receives an AR-11
   a. Update the relevant systems with the address information; and
   b. Forward the form to the Harrisonburg File Storage Facility.
   c. If the new address is a foreign address, interfile the foreign address change into the alien's record.
   d. If an address change includes correspondence, send the requestor an AR-11 with the filing instructions and forward the correspondence for inclusion in the respective file.
   e. If the correspondence contains information or a request for action in addition to the address change, you must
      i. Update any relevant systems with the address information;
      ii. Make a copy of the address change information, stamp the copy "Action Completed," and forward to the Harrisonburg File Storage Facility; and
      iii. Process the original correspondence as usual.
4. If your office receives returned mail, it must be processed within three (3) working days. The action official must check applicable systems for a recent address change.
   a. If a new address is found, the action official must
      i. Update applicable systems, and
      ii. Forward mail to the new address.
   b. If there is no system to update or the system will not accept an update
      i. Stamp or annotate the undeliverable mail;
      ii. Indicate that no system update was possible; and
      iii. Route returned mail according to your local mail procedures.
5. Example of filing instructions to be sent to the submitter:

   We received your change of address request. In order to completely process your address changes with the Department of Homeland Security (DHS); you must also complete an AR-11 form and mail it to the address below:

   Harrisonburg File Storage Facility

ATTN: AR-11
1344 Pleasants Drive
Harrisonburg, VA 22801

Every person over the age of 14 who is not a citizen of the United States or in "A" or "G" nonimmigrant status must complete a Form AR-11 within 10 days of the address change. Where possible, please provide an A-number (from your alien card) or other identifying numbers. Failure to complete all applicable sections may delay processing of the form.

Please disregard this notice if you have submitted an AR-11 form to DHS/USCIS within the last two weeks.

You may obtain additional copies of the AR-11 form on our web site at http://www.uscis.gov/or by contacting our National Customer Service Center at (800) 375-5283.

6. Local change of address forms
   a. Do not use or create locally designed forms to collect address change information.
   b. Aliens must use the AR-11 or AR-11SR in order to comply with the law on changes of address. The forms are available on the Immigration site and from these links:
      i. AR-11, Aliens Change of Address.
      ii. AR-11SR, Aliens Change of Address – Special Registration.
   c. When an office receives letters with changes of address, they must send a letter and an AR-11 form to the alien informing them that an AR-11 is required for an official address change. An example of the letter is located above.

Chapter 5 - Interfiling Classified Material

1. Records personnel may receive classified materials for interfiling into an existing file either through incoming mail or directly from an approved USCIS office. Items received from another FCO must have a completed Form 11000-11, Record of Transmittal for Classified Documents or Other Accountable Material attached.
2. When handling classified interfiling material from another FCO or outlying site, a cleared, qualified individual must:
   a. Receive the classified material directly from cleared field office staff;
   b. Review the accompanying Form 11000-11 to ensure that the material received is consistent with the listing of the material that was transmitted;
      i. If there are no discrepancies, sign and date Form 11000-11; place a copy in the office safe area; and return the original to the originating office.

ii. If the received material does not match the description of material on Form 11000-11, contact the sender immediately to initiate efforts to account for material that is potentially lost. If efforts to locate the information prove unsuccessful, a SIR must be filed.

c. Ensure that the appropriate classification cover sheet is attached to each classified document to be interfiled.
   i. Classified material used in making a decision in accordance with 8 CFR 103.2(b)(16)(iv) must be placed on the inner right side of the file jacket in a brown envelope marked Classified Material Used in Decision on (Type of Application or Petition). Include the subject's name, the file number, and the appropriate security classification on the envelope.
   ii. Classified material not used in making a decision must be placed in a brown envelope marked "Information Not Material in Making an Adjudicative Decision." Include the subject's name, the file number, and the appropriate security classification of the envelope.
d. If the file is unclassified or is classified at a lower level than the material to be interfiled, take it to the Security Officer for stamping with the proper (highest) classification.
e. The file may not be returned to storage until it is properly marked with the correct classification.
f. Refile the material in a proper GSA-approved security storage container.

Chapter 6 - Correspondence Filing

1. Correspondence between USCIS and aliens or their representatives must be filed in the respective A-file, Receipt file, or Alpha file only if it is needed to make a current or future adjudicative decision.
2. Before correspondence is routed or filed, it must be stamped or annotated to show the action is complete.
   a. If the letter asks for status, file it in a correspondence file after it has been answered.
   b. If the letter contains change of address information, process it in accordance with the change of address chapter.
3. The action complete stamp or annotation must show the initials and FCO/Unit of the person who completed the action and the date the action was completed.
4. If the correspondence does not pertain to a specific petition or application, it must be placed in the appropriate correspondence file of the office making the response. In most cases, this is the Field Office Subject Files – Correspondence.
5. If the correspondence does not require a response and falls into one of the five types of correspondence in the Uniform Subject Filing System Memorandum, you must follow the retention/destruction schedule outlined in this memo.

a. General Public Non-Action Mail: this is not the same as non-action material. This is mail that does not require a written response because it falls into one of the three categories listed below. General public non-action mail consists of:
b. Letters from persons or interest groups to express a point of view;
c. Campaign mail of standardized letters expressing a point of view; and
d. Derogatory mail.
e. Retain 90 days, and then destroy in accordance with NC1-85-83-11/1. All offices may use this series.
f. Congressional Correspondence: records consisting of correspondence between the USCIS and members of Congress concerning matters relating to the administration and/or enforcement of the Immigration and Nationality Act, laws and regulations, and constituent inquiries. Cut-off at the end of the calendar year; transfer to the FRC after one year. Destroy when five years old in accordance with N1-85-91-01/1. Any office may use this series.
g. Field Office Subject files – Correspondence: all correspondence, except policy, filed in general subject files of administrative nature between offices of USCIS, and with other governmental agencies, and with the general public, concerning matters relating to the administration or enforcement of the Immigration and Nationality laws and regulations, not part of any case file, and are to be classified as "C" correspondence. Destroy when one year old, exemption not to exceed three years in accordance with N1-85-80-06/2. This series is used in field offices.
h. Administrative Correspondence files: all correspondence, except policy, filed in general subject files of an administrative nature between offices of this service, other governmental agencies, and general public, concerning matters relating to the administration or enforcement of the Immigration Nationality laws and regulations, not a part of any case file. Retain one year in accordance with disposition authority II-NNA-101/2. This series is used primarily in headquarters' offices.
i. Public Inquiries: records consisting of correspondence sent by the public to Headquarters, USICE, USCIS, or USCBP or referred to DHS by the White House or the Attorney General. Cut off at the end of the calendar year; transfer to the Washington National Records Center (the NARA Federal Records Center in Suitland, MD) after one year. Destroy when five years old in accordance with N1-85-91-02. Only headquarters offices use this series

6. Headquarters subject files contain administrative and policy files of the USCIS containing information relating directly to individual aliens but are not part of any case file.
   a. These files are classified as "P" policy.
   b. They document enforcement and administrative duties and responsibilities assumed by the DHS as it carries out its mission through operational programs in adjudication and nationality, inspections, investigations, and detention and deportation, as well as the United States Border Patrol.
   c. Arranged by internal subject file classification.

d. Permanent- transfer to NARA in accordance with N1-85-01-01.
e. Used by any office.

7. Files must be labeled by file series, type, and year. A lead folder must precede each set of folders for each year and series.
   a. The lead folder must display:
      i. Series title;
      ii. Disposal Authority Number or General Records Schedule Number;
      iii. Year;
      iv. Date of retirement (if applicable); and
      v. Date of destruction.
   b. The follow-up folders must display:
      i. Series title;
      ii. Year; and
      iii. Folder contents.
   c. Example

Administrative Correspondence Files II-NNA-11/2 2002 Destroy Jan. 2004
Administrative Correspondence 2002 Reply to Status Inquiries January
Administrative Correspondence 2002 Reply to Status Inquiries February

Chapter 7 - Returning original documents

1. Original documents submitted in response to a request for an immigration benefit, must be returned to the petitioner or applicant upon completion of the adjudication. See 8 CFR 103.2 (b)(5).
2. Original documents submitted in response to a removal or enforcement action must be retained until the action is resolved. See Section 14.
3. USCIS form instructions state that original documents that are submitted when not required or requested will not automatically be returned and may remain a part of the record or destroyed after ingestion into ELIS. However, offices are encouraged to return voluntarily submitted original documents.
4. Original documents that we do not request or require and are submitted in conjunction with a physical application becomes part of the physical record and are retained in accordance with the applicable retention schedule. See 8 CFR 103.2(b(1).

5. Original documents that we do not request or require, submitted in conjunction with Form I-130, Petition for Alien Relative or Form I-140, Immigrant Petition for Alien Workers, that become part of a Receipt file may be destroyed pursuant to the applicable retention schedule.

6. The following documents submitted in conjunction with an ELIS application will be returned to the customer by USCIS or the Lockbox after ingestion into ELIS:
   a. Passports (US and foreign) and
   b. All other documents that appear to be foreign or issued by a foreign government.

7. The following exceptions apply to returning original documents submitted in response to a request for an immigration benefit:
   a. If we suspect that an original document is stolen, counterfeit, altered, or presented by an imposter, or is otherwise necessary for an investigation, then the original document must NOT be returned, pending further review by ICE. If the original document is confirmed as stolen, counterfeit, altered, or presented by an imposter, it must NOT be returned. Valid original documents should only be returned to the applicant once the investigation is complete, and the individual is not subject to removal.
   b. USCIS may destroy an original Form I-551, Permanent Resident Card, in conjunction with an approved Form I-90, Application to Replace Permanent Resident Card, pursuant to guidance in the Safeguarding Secure Forms Instructional Handbook.
   c. USCIS may destroy USCIS produced card documents, non-card documents, and certificates returned to USCIS if they are (see DAA-0566-2014-0005):
      i. Returned to USCIS from customer;
      ii. Returned to USCIS as found, unable to return to the owner;
      iii. Returned to USCIS as expired; or
      iv. Items created with flaws or inaccuracies; and
      v. Destroyed in accordance with guidance in the Safeguarding Secure Forms Instructional Handbook.
   d. Any original documents returned to USCIS as undeliverable will be stored for a period of one year from the date of receipt by USCIS before being destroyed.

8. If USCIS does not return an original document within a reasonable time after completion of the adjudication, the petitioner or applicant may request return of the original document by submitting a properly completed and signed Form G-884, Request for the Return of Original Documents.

9. When an office receives a request for the return of original documents, the Records Office must make sure the request meets the following standards:
   a. If the requestor does not appear in person, the G-884 must be notarized;
   b. If the request is submitted by a third party, the third party must have a legal relationship to the person whose documents they are requesting. Proof of the legal relationship must accompany Form G-884 per the form instructions; and

c. Documents in a foreign language have to be accompanied with a certified translation in English and a certified statement from the translator that he/she is competent to translate and that the translation is accurate.

10. If an original document cannot be returned for any reason, the responding office should notify the requester by sending Form G-885, Request for Additional Information to Obtain Original Document, and selecting the "other comments" option on the form and noting that the original document cannot be returned at this time.

11. Original documents must not be forwarded to the issuing country's embassies or consulates. as this could place current or future applicants for asylum, refugee, or other protected status in potential danger.

12. If an office receives a request for original documents based upon a Mutual Legal Assistance Treaty (MLAT), you must refer the request to USCIS local counsel.

13. Requests for return of an original document from a digitized file should be referred to the NRC Information Liaison by emailing IMLSINFO@uscis.dhs.gov or mailing:
Attention: External Agency Support
National Records Center
Information Management and Liaison Section
150 NW Space Center Loop
Lee's Summit, MO 64064

14. Confiscated original documents
    a. If USCIS suspects that an original document is stolen, counterfeit, altered, or presented by an imposter then the original document, sent to ICE for examination, may not be returned.
    b. If an original document is necessary for an investigation, removal action, or enforcement action, then the original document sent to ICE for examination may not be returned, pending further review by ICE.
    c. If an original document is confirmed as stolen, counterfeit, altered, or presented by an imposter, it must not be returned.
    d. Valid original documents may only be returned to the applicant once all investigations are complete and the individual is not subject to removal.
    e. Confiscated original document must be placed inside of an evidence bag that is clearly labeled as one of the following:
        i. Pending Document Review;
        ii. Valid - return to alien;
        iii. Counterfeit;
        iv. Altered;
        v. Imposter;
        vi. Pending Investigation;
        vii. In Removal Proceedings;

viii. Removal Proceedings Terminated - return to alien.

15. Requests for identity documents not contained in an evidentiary envelope
    a. Locate the requester's A-file and pull it.
    b. Review the A-file and verify that the document requested is in the file. If the requested document is an original and it is not needed to adjudicate a pending application for benefits, copy the document and have it certified as a true document to determine benefits.
    c. Put the certified copy in the A-file along with the completed G-884. On the G-884, note the date the original document was returned and initial the G-884.
    d. Prepare a cover letter for the signature of the Records Supervisor or another designated authority. Once the cover letter is signed, mail the letter and the document(s) to the requester. Send the package certified, return receipt requested.
    e. Change the A-file to a pending responsible party until the office receives a return receipt showing the requester received the document.
    f. When the return receipt comes back, file it in the A-file with the G-884. The A-file can then be shelved.

Part F - Requests for Immigration Records from Outside DHS

Chapter 1 - Requests from Outside Agencies to Review Immigration Records

1. USCIS immigration records and their contents belong to DHS and are managed in accordance with the Homeland Security Act of 2002.
2. Immigration records are primarily received and maintained by USCIS, ICE, and CBP. Additionally, the DHS Office of the Inspector General (OIG) may receive and maintain original immigration records if a certified true copy cannot meet their law enforcement or investigatory needs.
3. When Federal, State, or local law enforcement entities outside of DHS need information from our records, an authorized USCIS employee provides copies of the contents and certifies them as true in accordance with immigration policies and regulations. See RPM Vol 3, Part F, Chapter 4
4. Agencies outside of DHS may also be permitted to locally review an immigration record for the following purposes:
    a. Law enforcement; and
    b. A routine use as described by the specific Privacy Act notice for the type of record requested.
5. An agency outside of DHS requesting access to immigration records must send a memorandum in advance on official letterhead signed by their local director directed to the Chief of IIMD along with an accreditation list.

a. The accreditation list must have the following information on each individual from their agency who will be authorized to review USCIS records:
    i. Name;
    ii. Title;
    iii. Badge number (or other identifier); and
    iv. Clearance level.
b. Agencies must update their list annually or when there is a change to the information on the current list. The Records Custodian should notify agencies if their current list has expired.
c. The requesting office must be working in conjunction with a sponsor office with access to RAILS.
d. The requesting office must work with its DHS Point of Contact (POC) and local FCO to establish an RPC in RAILS.
e. All records and record movement must be tracked in RAILS.
f. Access to all records must be restricted to persons with a legitimate business need-to-know with appropriate background checks and clearances.
g. Requests must contain:
    i. Justification including description of how the records are needed to satisfy a mission-critical need, such as a large-scale investigation;
    ii. Duration of custody;
    iii. Transportation plan covering both the transfer to the requesting party and the return to USCIS; and
    iv. Designation of a DHS POC, a DHS alternative POC, and a POC for the non-DHS office that will receive the immigration records.
h. The requesting office must adhere to USCIS Records policies as codified in the RPM.
i. USCIS will not release classified files as part of an individual or multiple file request. For information regarding classified file requests, see RPM Vol 3, Part D, Chapter 1.
j. Immigration records must be stored and maintained in an area that is:
    i. Secure and climate controlled;
    ii. Restricted from sharing with other parties;
    iii. Protected from possible fire and water damage; and
    iv. Safeguarded from insects and rodents.
k. The requesting office must ensure all files are available to DHS in the event of a National Security Event (NSE) as outlined in RPM Vol 6, Part B.
l. The requesting office will provide status updates to the DHS POC on a consistent basis as defined in an agreed-upon communications plan.
m. IRIS Headquarters must approve the request.
n. Immediately report any loss, theft, concerns, or significant damage to immigration records to IIMD/PAB.

6. If a state or local agency wants to access records for reasons other than law enforcement or a routine use described by the Privacy Act notice for the records, they must file a FOIA request.

7. Requests for individual's immigration status must be directed to the Systematic Alien Verification for Entitlements Program (SAVE). This includes:
   a. Agencies outside of DHS, including law enforcement;
   b. Office of Personnel Management (OPM) Special Investigators conducting background investigations;
   c. OPM contract investigators conducting background investigations;
   d. Investigators working on behalf of agencies with delegated authority; and
   e. The public

8. Any requests for immigration information or records must not be completed or researched by the individual under investigation.

9. When a naturalized United States citizen needs a Certificate of Naturalization "authenticated" by the U.S. Department of State for a foreign government, USCIS provides a certified true copy. "Authentication" is a term used by the U.S. Department of State and other Governments to describe what USCIS refers to as Certified True Copies. When a Certificate of Naturalization is required to be authenticated, use the term "Certified True Copy."

10. In an emergency, the Records Supervisor or the District Director (or other Field Office Director) may allow immediate access to a record which is available locally.
    a. The requesting agency must provide the following information via phone, a letter, fax, or email:
       i. Name of the individual in the requested record;
       ii. A- or Receipt-number for the requested record;
       iii. Place and date of birth for the individual in the requested record;
       iv. Name and phone number of the requestor (who must be on the accreditation list); and
       v. Justification for accessing the information.
    b. The Records Custodian will carefully review the request and determine if the record(s) can be disclosed.
    c. DHS is permitted to disclose Privacy Act information without the consent of the subject under certain conditions; however, USCIS is not required to make disclosures to non-DHS investigators. USCIS Records Custodians shall make the decision to disclose records upon a finding that the requestor is a lawful authority and requires a justifiable need for access to the record(s). See 5 U.S.C. 552a (b) .

11. If needed to protect the confidentiality of an investigation, an agency can make a request to access immigration records directly to the District Director, Service Center Director, or Officer-in-Charge, rather than the Records Custodian. If the request is denied, a copy of the proposal and denial can be sent to Headquarters, General Counsel for approval.
12. Verbal denials are sufficient. The requestor may appeal a denial by providing additional information or going through the chain-of-command from the local level through the Region (if applicable) to IIMD.

Chapter 2 - Outside Agencies Reviewing Immigration Records

1. If the request to review the immigration record is approved
   a. The Records Custodian must schedule an appointment with the requestor to review the file.
   b. The Records Custodian, or designated representative, must remain in the room with the reviewer to ensure that nothing is removed from the file and to answer any questions that might arise.
   c. The Records Custodian may assist the requestor with the record to include making copies if requested.
   d. The requestor must complete Form G-658, Record of Information Disclosure (Privacy Act) after reviewing the file if:
      i. The subject of the file is an LPR or a U.S. citizen; or
      ii. The requester is from an agency outside the DHS.
   e. A copy of the G-658 must be filed in the subject's record. Although not required, an office may choose to retain an additional copy of the G-658 for local record-keeping purposes.
2. Onsite review of classified materials
   a. If a request is received from another government agency to review a classified file (for example, OPM or FBI), records personnel must ensure that the requestor has a need to access classified information in the performance of their assigned job duties. This should be indicated by a formal request from the requestor's supervisor on their official agency letterhead.
   b. Confirmation of their security clearance must be provided to the OSI Personnel Security Division (PSD) for approval to handle classified NSI. To contact OSI PSD to initiate a records check or to obtain further information, please email Customer Service.
   c. The requestor from another agency is not authorized to see documents from a different agency/third party agency. Documents such as these should be removed prior to allowing the requestor to view the file.
   d. The requestor must fill out Form G-658.
   e. Once a classified document goes into a file, the entire file becomes classified at the highest level of classified NSI contained within. If practicable, the needed classified documents can go into a T-file, and the T-file can be reviewed instead of the A-file.

f. Review of the file should take place in an area that is not open. Only personnel classified at the level of the file on review should have access to the area.
g. If copies of documents are needed, the requestor should inform records personnel so the copies can be made on a machine accredited by OSI for the reproduction of classified documents.

Chapter 3 - Outside Agencies Requesting Original Documents

1. In general, USCIS will not release original documents to outside agencies. A certified true copy will be provided in lieu of the original.
2. If absolutely essential, original documents from an immigration record may be provided for forensic laboratory analysis.
3. Requests for original documents must be in writing and provide:
   a. A list of specific documents requested and
   b. Justification of the need for each document.
4. Upon review and approval of the request for an original document, the Records Custodian must
   a. Make a certified true copy for the file;
   b. Attach Form G-24, Certification of Documents; Form G-658, Record of Information Disclosure (Privacy Act) (if applicable); and a copy of the request including justification for the records to the certified true copy;
   c. Give the original documents directly to the requestor or send by traceable mail; and
   d. Provide a copy of the G-658 to the local Legal Office if
      i. The subject of the record is an LPR or a USC; and/or
      ii. The requestor is from outside of DHS.
5. Access to records in the FRC
   a. The FCO should request retired files for an outside agency to view locally.
   b. Only IIMD may grant access for outside agencies to review records at the FRC.
   c. In an emergency, the NRC may pull records from the Lee's Summit FRC and grant access to review the record at the NRC, Information Liaison Division.

Chapter 4 - Certified True Copies

1. Certification procedures discussed in Chapter 3 of this Part apply to paper, electronic, and hybrid paper-electronic records, as well as retired records. Users can create a certified paper copy of the digital record using the Enterprise Document Management System (EDMS), Electronic Immigration System (ELIS), and STACKS.
2. A certified copy, not the original, should be provided for court proceedings. See 8 U.S.C. 1443(f).

3. In accordance with 8 CFR 103.7(f), the following officials may certify records when the files or documents are in the custody of their offices:
   a. Chief, IIMD;
   b. Regional Directors;
   c. District Directors;
   d. Field Office Directors;
   e. Service Center Directors;
   f. Director, NRC; and
   g. Director, NBC.
4. Any official authorized to certify records may designate others to certify records as long as the designation is in writing, and the office maintains a copy of the designation memo.
5. Requests for certified true copies must be directed to the local FCO.
6. Certified true copies must:
   a. Be paginated;
   b. Contain copies of all requested pages, front and back, except for third-party agency or other government documents (not including Department of State visa packets and Identity History Summaries, formerly known as Rap Sheets); and
   c. Include Form G-24, Certification of Document embossed with the official seal and a cover memorandum (see sample document).
7. How to certify an A-file
   a. Direct requests for certified true copies to the local File Control Office (FCO).
   b. When providing a certified copy of the complete file, paginate each page of the file prior to copying.
   c. If the request is for only a specific document or documents from the A-file (for example, a petition and supporting documents or an application for benefits), review the file for the requested documents. Paginate the requested documents in the A-file and the certified copy.
   d. Certain records of other federal agencies that are a part of a USCIS file must be protected from unauthorized disclosure. Do not copy reports or correspondence originating from another federal agency.
   e. Replace pages originating from another government agency with blank sheets labeled only with the name of the agency. Personnel performing records management functions are not expected to read each document in the A-file. If they can clearly identify a report/correspondence as belonging to another federal agency, they should not copy it.
   f. Paginating should continue on the blank pages.
   g. Multiple page documents must have a blank page for each page withheld. Label each page with the name of the agency.

h. Identity History Summary (formerly known as RAP sheet) or forms owned by other agencies and completed by petitioners (for example, forms contained in Department of State visa packets) are not categorized as reports or correspondence and therefore do not fall under this provision.

i. Certification: Prepare Form G-24, Certification of Document and a cover memorandum (see sample document).
   i. Emboss the G-24 with the official seal.
   ii. Fasten the cover memorandum securely on top of the package contents.
   iii. If the certified copy provides only specific document(s) from the A-file (for example, a petition and supporting documents or an application for benefits), annotate the G-24 with a description of the document(s) provided.

j. When responding to a request for a certified copy of an A-file, personnel performing records management functions must copy the entire A-file (except third-party agency documents). If the requester or other party in receipt of the certified copy needs to remove or redact any documents after the A-file copy has been paginated and certified, it is incumbent upon the requester to annotate the G-24, Certification of Documents, accordingly.

k. Some certifications may only require verification of electronic data and the physical file is not required (such as a certified copy of certificate of naturalization).

l. Upon receiving a valid request, check RAILS to determine file location. If needed, request the file.

m. Review the file for the requested documents. Make a copy of the documents found:
   i. Ensure the copies are fully legible and a complete reproduction of the original.
   ii. Copy both front and back if there are any annotations or markings.

n. If you do not find the requested document (s), notify the requestor.

o. If your office does not have an embosser with an official seal, submit a request through your chain of command to obtain one. It is not necessary to emboss each page of the copied file.

8. When a naturalized US citizen needs to have a Certificate of Naturalization authenticated, USCIS will copy the document and certify it as a true copy.
   a. If the applicant has the original certificate, the applicant must request the certification from their local USCIS office.
   b. If a USCIS Headquarters program office needs a certification, the office must request via the Office of Records Management (ORM) website.

9. To certify a record that has been digitized in EDMS, follow the detailed instructions in section II.4 of the Using the Digitized A-File CD guide entitled "Using the Certified Copy Export," ensuring the copy complies with the requirements outlined in this chapter.

10. Only the Attorney General is authorized to make and issue certifications of any part of the naturalization records of any court. That authority is delegated to USCIS and allows only designated USCIS officers to certify naturalization records or Certificate files of the Service or the court. See 8 U.S.C. 1454
    a. Naturalized persons may obtain certified true copies of Certificate files as instructed on the USCIS website.
    b. USCIS has no authority to issue certified true copies of naturalization records to third parties.
11. All requests for certified true copies of immigration records at NARA should be sent directly to NARA.
    a. If the FCO code is NMO (NARA Archives Kansas City), inquiries can be sent to Elizabeth Burnes or:
    Archivist
    National Archives, Kansas City
    400 West Pershing Road
    Kansas City, MO 64018
    b. If the FCO code is NCA (NARA Archives San Bruno), inquiries can be sent to Michelle Bradely or:
    Archivist
    National Archives, San Francisco
    1000 Commodore Drive
    San Bruno, CA 94066
    c. Requests must include the A-number, name of the individual, and if possible the accession and box number. Access to accession information can be found in the Archival Research Catalog (ARC). A successful search in ARC can be completed by searching on the A-number (in the format A1234567) or an individual's name.

Chapter 5 - Requests for Historical Records

1. In the absence of an A-file, COW can produce the following official files for the purpose of verifying status:
    a. Files documenting Legal Permanent Resident (LPR) admission: Visas files, 1924-1944 and Registry files, 1929-1944.
    b. Files documenting Naturalization/Citizenship: C-files, 1906-1956.
    c. Alien Registration Forms, 1940-1944 (Form AR-2): AR-2 forms do not in themselves document LPR admission. Information shown on the form was provided from the subject's memory and not verified by the agency. Information on the form may provide data needed to locate an official admission record. See General Counsel Opinion 93-70.
2. USCIS does not process requests for records not in our custody.
3. All public requests for immigration records at NARA, for example public requests related to genealogy, return of original documents, or FOIA, must be directed to NARA.

a. USCIS employees must not make requests of NARA for documents on behalf of the public.
b. Do not advise the public to file a FOIA request with NARA, as NARA handles most requests outside the FOIA/PA process. If NARA's FOIA/PA provisions apply to the request, NARA will advise the researcher concerning proper submission.
c. If the FCO code is NMO (NARA Archives Kansas City), inquiries can be sent to Elizabeth Burnes or:
Archivist
National Archives, Kansas City
400 West Pershing Road
Kansas City, MO 64018
d. If the FCO code is NCA (NARA Archives San Bruno), inquiries can be sent to Michelle Bradely or:
Archivist
National Archives, San Francisco
1000 Commodore Drive
San Bruno, CA 94066
e. For more information regarding immigration records in NARA custody, see NARA.

4. The USCIS Genealogy Program has published general descriptions of the agency's historical records as defined in 8 CFR 103.39.
a. If contacted by researchers seeking information on genealogy records, direct them to the USCIS Genealogy Program .
b. If contacted with customer complaints regarding the Genealogy Program, forward the information to the Genealogy Program mailbox or send them by mail to:
USCIS Genealogy Program
1200 First Street NE Room 230
Washington, DC 20529-2206

5. The USCIS Historical Library publishes guidance on researching historical records of individual immigrants as well as for those researching historical topics (events, places, policies). For more information or assistance in locating agency records, email the USCIS Historical Library or call 202-272-8370.

Chapter 6 - Certificates of Nonexistence

1. A Certificate of Nonexistence is an official USCIS record certifying that no record exists on a particular individual, decision, or action based on the identifying information or criteria provided by the requestor as a result of our electronic and physical searches.

2. The authority to provide a Certificate of Nonexistence of USCIS records is outlined in 8 CFR 103.7(f). The following officials or their designees, authorized in writing, may certify records when the files or documents are in the custody of their offices:
a. Chief, IIMD;

b. Regional Directors;
c. District Directors;
d. Field Office Directors;
e. Service Center Directors;
f. Director, National Records Center (NRC); and
g. Director, National Benefits Center (NBC).

3. Requests for Certification of Nonexistence must come from ICE, CBP, or USCIS in the form of an official memorandum to the appropriate supporting Records office. The request should include the following:
   a. Requestor's name, title, organization, contact number, fax number, e-mail address, and mailing/shipping address;
   b. Type of certificate being requested (for example, Form I-212, Application for Permission to Reapply for Admission into the United States after Deportation or Removal; no record of naturalization; no record) and date of request; and
   c. Subject information-complete name, date of birth, country of birth, file number, date of deportation, and any aliases.

4. Certifications of Nonexistence are granted in response to:
   a. Requests by DHS employees and other government agencies authorized to make the request - such as investigators, special agents, or attorneys;
   b. Requests by customers for a certificate of nonexistence of naturalization as a citizen of the U.S.; or
   c. Verification that no records (file or systems information) exist for the individual, action or decision.

5. Certifications of Nonexistence will state one of the following:
   a. After deportation the person was not granted permission to reenter the U.S.;
   b. There is no record of Naturalization as a citizen of the U.S.; or
   c. No records (neither a file nor systems information) exist for the individual/decision/action.

6. Process Part I: local offices
   a. The local Records office performs thorough searches of the databases listed below to determine and locate all possible files/records associated with the subject:
      i. Central Index System2 (CIS2);
      ii. Computer-Linked Application Information Management System (CLAIMS); and
      iii. Enforcement Alien Removal Module (EARM).
   b. The local Records office should request, review, and obtain all files/records that relate to the subject. These may include:
      iv. Immigration File Basics;
      v. T-files;
      vi. Sub-files; or
      vii. Receipt files.

c. The local Records office should work with the official requesting the certificate to review records, consolidate files, and perform required systems updates. If during the review of files or databases, (in the case of a search for a person) additional aliases for the individual are discovered, please work with the requester to resolve. Add any new pertinent aliases to the original request for a certificate of nonexistence and search the databases under each of the new aliases.
d. If the system searches result in a "no record" found on the subject sends a request to HQ IIMD, Records Services Branch to request a special manual search be performed for a certificate of nonexistence of an official agency record.

7. Process Part II: forwarding requests to HQ IIMD
   a. If DHS Offices are not able to find A-file information in CIS2 on applicants who were born and entered the U.S. before December 31, 1975, certifications requests can be submitted through the ORM Request website. To obtain the user guide with instructions and a link to the ORM Request website, please follow the instructions below:
      i. Send an e-mail to Certificateofnonexistence@uscis.dhs.gov e-mail box with "Instructions" on the subject line of the e-mail.
      ii. An automated response will be generated with the subject line "User Guide for the ORM Request Web Site".
      iii. The "User Guide for the ORM Request Web Site" contains an overview of the web site, step-by-step instructions on how to create an account to access the web site and how to submit requests.
   b. Processing time for requests is based on the volume of work pending.
   c. Both COW RECORDS and the field can perform all other requests.

Chapter 7 - Checks for Expatriation

1. Expatriation is the loss of citizenship that occurs as the result of a citizen voluntarily performing an act of expatriation with the intent to relinquish citizenship as set forth in the Immigration and Nationality Act. The most common acts of expatriation include the following:
   a. Naturalization in a foreign state;
   b. Taking an oath or making an affirmation of allegiance to a foreign state;
   c. Service in the armed forces of a foreign state;
   d. Employment with a foreign government; and
   e. Taking a formal oath of renunciation of allegiance before a U.S. consular or diplomatic officer.

2. If you have any question about any aspect of loss of nationality, see the State Department Web site, the nearest U.S. Embassy or Consulate, or the
   Director, Office of Legal Affairs, Overseas Citizen Services
   U.S. Department of State
   CA/OCS/L, SA-17, 10th Floor

Washington, D.C. 20522-1707

3. When an American Consul determines that a person has become expatriated, a Certificate of the Loss of the Nationality of the United States (generally referred to as a Certificate of Expatriation) is furnished to DOS' Passport Office, who provides a copy to DHS/USCIS/IRIS/NRC.
   a. All certificates must be forwarded to the following address for proper processing:
   Attention: External Agency Support
   National Records Center
   Information Management and Liaison Section
   150 NW Space Center Loop
   Lee's Summit, MO 64064
   b. NRC receives the certificates and
      i. Updates CIS2 to show the COA as Expatriation;
      ii. Marks the certificate as Action Completed;
      iii. Forwards the certificate to the office with the A-file for interfiling; and
      iv. Creates an A-file if no previous file exists.
   c. For questions on the process, contact expatriation.cases@uscis.dhs.gov.
4. Generally, checks on expatriation are initiated by an adjudicator or investigator when:
   a. The U.S. nationality of a person is material to processing a case or
   b. That person has been absent from the United States for an extended period of time, or under circumstances which raise a question as to whether that person may have become expatriated.
5. If a review of an A-file for expatriation yields no results, and
   a. The CIS2 History Screen does not show a record; and
   b. The expatriation was prior to 1975; then
   c. Request that NRC review microfilmed naturalization records via manual search request through the ORM Request website. The request must include enough information to properly process, such as:
      i. Name;
      ii. Date and place of birth;
      iii. Manner in which United States nationality was acquired;
      iv. Present residence; and
      v. All facts that indicate that the person may have become expatriated.
6. If the expatriation was after 1975 and no record of expatriation was found, make a direct inquiry to the Department of State or the appropriate American Embassy or Consulate.
   a. If the person whose nationality is in doubt is in the United States, address the inquiry to the Director, Passport Office, Department of State, Washington, DC 20524.
   b. If the person is outside the United States, send the inquiry directly to the appropriate Embassy or Consulate. See the State Department web site (www.state.gov) for address information.

Chapter 8 - Naturalization Revocation

1. If a naturalized citizen's citizenship is revoked, notification must be sent to the NRC.
2. An electronic copy of the court's Order of Revocation must be sent to IMLSINFO@uscis.dhs.gov so that NRC can update the status in CIS2 (9317).
3. Any original certificates must be sent to the NRC indicating whether or not you have sent an electronic copy. Mail to the following address:
   Attention: External Agency Support
   National Records Center
   Information Management and Liaison Section
   150 NW Space Center Loop
   Lee's Summit, MO 64064
4. All certificates recovered as a result of an Order of Revocation must be voided by drawing a diagonal mark on the face of the certificate and writing "VOID" across the face of the certificate.
5. The voided certificate must be copied. The copy must be placed in the file and the original must be destroyed per Office of Security and Integrity (OSI) secure form procedures.

Part G - Retention/Destruction/Retiring Immigration Records

Chapter 1 - Retention of Immigration Records

1. Immigration records must be retained and disposed of according to their retention schedules. For additional information on record schedules, see RPM Vol 1, Part D.
2. A-files are permanent records that are sent to the NRC upon closure. The NRC prepares the records for retirement and accession to NARA. See A-file retention schedule.
3. Other immigration records have different retention schedules and disposition procedures based on individual record schedules. For a list of all record schedules, see USCIS retention schedules.

Chapter 2 - Retiring Immigration Records

1. An A-file or Substitute-file (Sub-file) is eligible for retirement when one of the following actions take place:
   a. A Death Certificate or notification of death is received;
   b. A person is naturalized or a Certificate of Citizenship is issued; or
   c. DHS receives Form I-407, Abandonment of Lawful Permanent Resident Status, indicating that an individual has left the U.S. and does not intend to return.
2. The NRC is responsible for retiring non-classified A-files and Sub-files.

3. The NRC/Immigration Records Contract Management Section (IRCMS) is responsible for retiring all classified files at the Secret level and below.
   a. You must obtain approval for the shipment prior to mailing the files.
   b. To obtain approval, email the request to SecuredFilesSupport@uscis.dhs.gov and include the number of files to be retired and the approximate box volume.
   c. For additional information, refer to the Classified Files Quick Reference Guide.
   d. NRC/IRCMS is responsible for completing Form SF-135, Records Transmittal and Receipt and assigning corresponding accession numbers.

4. BOIB is responsible for retiring all classified files at the Top Secret level and files that have been recalled from retirement accessions/transfers.
   a. You must obtain approval for the shipment prior to mailing the files.
   b. To obtain approval, email the request to COWREC@uscis.dhs.gov and include the number of files to be retired and the approximate box volume.
   c. IIMD/BOIB is responsible for completing Form SF-135, Records Transmittal and Receipt and assigning corresponding accession numbers.

5. All other inquiries regarding classified retirement shipments should be sent to SecuredFilesSupport@uscis.dhs.gov.

6. Preparation of retired files
   a. Conduct a complete physical review of the A-file to determine its current status;
   b. Search the appropriate systems based upon the documentation in the file to ensure the case is closed and that accurate data is entered into the systems;
   c. Ensure that the individual has only one A-file. If another A-file is found, see RPM Vol 3, Part C, Chapter 4 Duplicate A-numbers; and
   d. If the status of the file cannot be determined, consult the responsible Operating Unit.

7. FCOs must forward A-files and Sub-files to the NRC for storage or retirement when there is no longer an operational need for the file. Prior to shipping the files to NRC for retirement, the FCO must ensure:
   a. All electronic systems are updated and accurate, including CIS2 and especially post-naturalization;
   b. There are no pending actions such as adjustments, naturalization, or an outstanding immigration bond;
   c. There are no stamps in the file, such as:
      i. M-125 Under Docket Control: Placed on a file when the subject of the file is placed under deportation docket control. This form should be removed by the operating unit when the action is completed.
      ii. Files with a Class of Admission 'PEN' may be retired if they meet retirement criteria, including 5 years of inactivity. The file MUST NOT have a currently active application/petition.
   d. The individual has only one file. If another file (including receipt files and T-files) is found, see RPM Vol 3, Part C, Chapter 6 for guidance on consolidations;

e. A copy of the Certificate of Naturalization or Citizenship (if appropriate) is in the A-file;
f. The barcode is readable and jackets are intact; and
g. The Year of Birth (YOB) is annotated with a black chisel tip marker (use 1" digits) on the front center of the file.

8. Ship files to the NRC at the address below. Boxes not clearly identified for retirement will be shelved instead of retired.
National Records Center
ATTN: Retirement Department
150 Space Center Loop
Lee's Summit, MO 64064

9. Temporary files (T-files), Receipt files, and Work files (W-files) can only be retired by the NRC.

10. Digitized Receipt files are held in EDMS for a predetermined amount of time based on whether the status of the Receipt file is accepted or rejected and whether any other Receipt files in the transaction are accepted or rejected. Receipt files will be removed from EDMS the evening of the Retention Expiration date.

11. If it is necessary to keep a Receipt file past the Retention Expiration date, a hold can be placed on the Receipt file. Please see the Placing a Retention Hold section of the EDMS User Manual for more information.

12. If an FCO has more files eligible for retirement than it can review or process at one time, files should be retired in segments with the oldest files being retired first.

13. Preparing A-files for retirement
    a. Conduct a complete physical review of the file to determine its current status relative to benefit or enforcement action.
    b. Search the appropriate systems based upon the documentation in the file to ensure the case is closed and that accurate data is entered into the systems.
        i. Verify the existence of the A-file in the Central Index System2 (CIS2) using ID Number Search (ID) Screen CIS2 9504.
        ii. Verify that the following information in CIS2 is correct:
            - Current FCO;
            - Name;
            - Date of birth;
            - Class of admission; and
            - Consolidation information, if applicable.
    c. If the status of the file cannot be determined, consult the responsible Operating Unit.
    d. A routing sheet must be included on top of the files in each box.

Chapter 3 - Actions Involving Retired Immigration Records

1. See RPM Vol 3, Part E, Chapter 2 for guidance on adding interfiling to a retired file.
2. If you have a file that needs to be consolidated or merged with a retired file, request the file from the FRC and then follow the guidance in RPM Vol 3, Part C, Chapter 6 regarding file consolidations.
3. When requesting a retired classified file from an FCO other than the NRC, the FCO will request the file as a permanent withdrawal from NARA. Once the action on the file is complete, the file is sent to the NRC for potential declassification and/or re-retirement.

Volume 4 - Systems

Part A - Systems Overview

Chapter 1 - Introduction

1. DHS owns and maintains the following types of systems:
   a. Record systems - used primarily to track and maintain records;
   b. Case management systems - used primarily to track and maintain applications and petitions for some type of benefit; and
   c. Enforcement systems - used primarily to track and maintain immigration enforcement actions.
2. USCIS has three (3) NARA-approved content management systems. Any partial or fully electronically filed elements of the ROP must be housed in one of these repositories:
   a. EDMS (Enterprise Management Document System),
   b. ELIS (Electronic Immigration System), and
   c. STACKS.

   No other system may be used for this purpose without IRIS' express approval. The ROP of a particular application or petition may not be interspersed among multiple electronic repositories; it must be contained within a single such repository.
3. The following chapters provide a brief overview of the most commonly used systems within DHS with an emphasis on systems of interest to people in Records and those maintained by IIMD.

Chapter 2 - Records Systems

1. CIS2 (Central Index System2) is the primary system used for storing and maintaining alien biographic, current, and historical immigration status information. The system maintains information on lawful permanent residents, naturalized citizens, U.S. border crossers, apprehended aliens, legalized aliens, aliens who have been issued employment authorization and other individuals of interest to the DHS. For more information and training, see CIS2 Connect site.
2. RAILS tracks the location of alien records. For more information and training, see RAILS Connect site.
   a. Notifications alert users if a user at a different FCO receives a record that is in their custody in RAILS.
   b. The first 10,000 records are downloadable from RAILS Reports or Widgets. For a full listing of all records, reports must be run from SMART.
   c. For more information on reports, see Reports Overview.
   d. For information on supervisor functions, see Supervisory Dashboard

3. CPMS (Customer Profile Management System) is the repository of biometric & background check data for USCIS. CPMS provides the capability to:
   a. Store and reuse biometric images and biographic information;
   b. Record biometric and biographic data collected by other USCIS systems;
   c. Perform biometric vetting;
   d. Send newly captured fingerprints to DHS-IDENT for verification against previously captured fingerprint images; and
   e. Request background checks from FBI and, depending on the form type, DoD or a foreign partner country.
4. ARCIS (Archives and Records Centers Information System) is the web-based IT system of NARA's FRCs. For more information on ARCIS, see ARCIS Quick Referencee Guide or the USCIS Records Officer Connect site.
5. VIS (Verification Information System) supports the Systematic Alien Verification for Entitlements (SAVE) program by providing automated status verification information to federal, state, and local benefit granting and entitlement agencies. For more information and training, see SAVE Connect site.
6. FIRST (FOIA Immigration Records SysTem) is a system used to track the progress of FOIA/PA requests nationally. FIRST replaced the Freedom of Information Act Privacy Act Information Processing Systems (FIPS). FIRST allows members of the public to make requests online, USCIS employees to digitally manage and process requests, and requestors to receive digital files from USCIS. For more information and training, see on FIRST visit FIRST Connect site.

Chapter 3 - Case Management Systems

1. The USCIS Electronic Immigration System (ELIS) is a web-based IT solution that streamlines and enhances USCIS's case management and benefits processing operations through automation.
   a. Personnel can request ELIS access via MyAccess.
   b. For additional information and training resources, see ELIS User Manual and other guides.
   c. ELIS is not authorized to store any LHMs:
      i. Classified LHMs must be viewed on the HSDN; and
      ii. Unclassified LHMs must be stored in the corresponding physical file. If a corresponding physical file does not exist, the LHM must be stored in a RAILS trackable W-file.

2. CLAIMS 3 LAN (Computer-Linked Application Information Management System 3 Local Area Network) or C3 assists in processing applications related to benefits and visas. It provides USCIS with a decentralized, geographically dispersed LAN-based mission support case management system, with participation in the centralized CLAIMS 3 Mainframe data repository. Originally developed to track the receipting of applicant/petitioner remittances and to produce notices documenting the remittance, CLAIMS 3 LAN functionality now includes adjudication, archive, card production, case history, case transfer, on-demand reports, electronic file tracking, image capture, production statistics, status update and electronic ingest of applicant data captured through the E- Filing web application and the Lockbox. For more information on CLAIMS 3, see C3 ECN site.
3. CLAIMS 4 (or C4) manages the processing of Naturalization cases. For more information on CLAIMS 4, see C4 Guide
4. EADS (Employment Authorization Document System)
   a. The Employment Authorization Document System (EADS) automates the entry and edit of applicant information, produces data cards for employment authorization documents, and produces denial documents supporting Form I-765, Application for Employment Authorization.
   b. Use CIS2 Screen 9213, Displaying Employment Authorization Document System (EADS) Data, to see the card information in CIS2.
   c. The 100 million A-numbers assigned by EADS are electronic files only, there are no hardcopy A-files.
5. WRAPS (Worldwide Refugee Admissions Processing Asylum, Parole System)
   a. RAPS provides full case tracking and management capability for all USCIS Asylum casework.
   b. RAPS interfaces with CIS2, EARM, and NAILS (National Automated Immigration Lookout System).
6. SEVIS (Student and Exchange Visitor Information System) is a web-based system that DHS uses to maintain information on SEVP (Student Exchange Visitor Program)-certified schools and the F and M students who come to the United States to attend those schools. SEVIS also maintains information on DoS-designated exchange visitor program sponsors and J-1 visa exchange visitor program participants.
   a. SEVIS enables schools and program sponsors to transmit electronic information and event notifications via the internet to USCIS and the Department of State for the duration of a student's or exchange visitor's stay in the United States.
   b. The system will reflect international student or exchange visitor status changes, such as admission at Port of Entry (POE), change of address, change in program of study, and other details.
   c. For more information, see SEVIS web site.

Chapter 4 - Enforcement Systems

1. ENFORCE (Enforcement Case Tracking System) is a case management system for DHS enforcement activities that integrates a collection of automated case management and functional systems for arrest bookings.
2. TECS and TECS by ELIS are web-based systems owned by CBP that provide access to a large database of suspect information and interfaces with a number of other law enforcement systems. DHS owned systems that facilitate inspection of applicants for immigration benefits.
3. NCIC (National Criminal Information Center)
   a. NCIC is a nationwide, computerized information system developed by the FBI to provide information concerning:
      i. Crimes and criminals of nationwide interest;
      ii. Stolen property information; and
      iii. Locator-type file for missing and unidentified persons.
   b. The main NCIC computer, located at FBI headquarters in Washington, DC, serves all criminal justice agencies on local, state, and federal levels. Each agency accesses NCIC through its federal or state system.
   c. USCIS receives NCIC results via TECS and TECS by ELIS.
4. MFAS (Marriage Fraud Amendment System) is a legacy mainframe-based case tracking system designed to support the adjudication of petitions covered by the Immigration Marriage Fraud Act (IMFA) of 1986. The system maintains records on eligible immigrant entrants, tracks cases, initiates and schedules interviews, accepts petitions from immigrants and spouses, generates routine correspondence, and produces management and statistical reports.
5. NAILS II (National Automated Immigration Lookout System II)
   a. The National Automated Immigration Lookout System II (NAILS II) is a mission-critical mainframe system used by DHS to determine a traveler's admissibility to the U.S.
   b. NAILS contains approximately 1.2 million lookout records, including data received from the Department of State and NIIS.
   c. NAILS records interface with TECS and CIS2. NAILS supports lookout search, primary and secondary inspection operations, lookout record maintenance, and system administration functions.
   d. NAILS adds a flag to CIS2. It will show up on the CIS2 9101 screen as the word NAILS under Other Information.
6. EARM (Enforce Alien Removal Module) is part of the ENFORCE Integrated Database (EID). It manages alien removal proceedings and integrates data from various parts of the EID. EARM supports case, docket, and custody management, and generates reports. The system links all encounters and cases related to a person using the person's A-number. It is a component that replaced the Deportable Alien Control System (DACS).

Part B - IIMD Systems

Chapter 1 - CIS2 (Central Index System)

1. CIS2 (Central Index System) is a repository of electronic data that summarizes the immigration history of an alien. It serves as the focal point for many USCIS systems to consolidate information about an alien requesting benefits.

2. Personnel must request CIS2 access via MyAccess complete CIS2 training prior to receiving access. CIS2 training is available via PALMS and from IIMD/IMTB. The MyAccess application provides support to create/update accounts for USCIS systems such as CIS2, RAILS and the Enterprise Document Management System (EDMS).
   a. ICE File Control Offices (FCO's), ICE Non-FCO's and CBP all have the ability to manage USCIS systems access rights through MyAccess.
   b. The request is automatically routed to the requestor's supervisor/approving organization group for initial approval/denial. The supervisor/approving organization group will also determine if requested restricted access rights (if any) are necessary.
   c. There are up to four levels of approval needed for access to CIS2 depending on the transaction requested.
      i. Approval 1 – First Line Supervisor/Approving Organization Group;
      ii. Approval 2 - Records Managers/DRM/Restricted Access Administrator (RAA)/FCO Admin for RAILS;
      iii. Approval 3 – Regional/ HQ Level Program Office; or
      iv. Approval 4 – IIMD.

3. Requestors must provide a copy of the training certificate to their immediate supervisor/approving organization group to confirm completion of training.

4. Certain transactions in CIS2 are restricted to a need-to-know basis based on business operations.
   d. Requests for restricted access are completed through MyAccess and will go through multiple levels of approval.
   e. Only Records personnel or persons performing Records duties (including contractors) and who have completed the CIS2 training may be granted access to restricted transactions. Each individual FCO will work with their respective Program Office to determine the maximum number of access accounts per FCO based on their business needs.
   f. Requestors have the opportunity to select from a list of restricted access permissions, (see chart below, not a complete list).

Code	Restricted Transaction Description
9301	New File Add (3)
9302	Verify New File (3)
9311	Natz Stub (2)
9312	Derivative Citizenship (2)
9314	Expatriation (4)
9315	Repatriation (4)
9316	Status Change (Class of Admission) – COA (4)
9317	Revocation of Naturalization (4)*
9411	Personal Description Data (4)
9413	Status History Change of Class (4)
9414	Natz Number Deletion (3)
9421	Delete All Data for a Person (4)
9427	Reverse 1367 Set in Error (4)
9428	Remove 1367 Confidentiality (4)
9506	File Transfer Privileged Request (3)

*Restricted to IIMD, NRC, and Historical Fingerprint Enrollment Office (HFE) only

5. Supervisors must use MyAccess to terminate CIS2 or TRKS access rights whenever an employee no longer needs access or whenever an employee separates from their assigned office/duties.
6. When a person uses CIS2 to request a record, CIS2 interfaces with RAILS and changes the File Transfer Request (FTR) status. This prompts the RAILS system to start generating pull tickets.
7. For more information on CIS2, see CIS2 Connect site.

Chapter 2 - CPMS

1. The Customer Profile Management System (CPMS) is the repository of biometric and background check data for USCIS.
2. CPMS provides the capability to:
   a. Store and reuse biometric images and biographic information;
   b. Record biometric and biographic data collected by other USCIS systems;
   c. Perform biometric vetting;
   d. Send newly captured fingerprints to DHS-IDENT for verification against previously captured fingerprint images; and

e. Request background checks from FBI, DOD, or a foreign partner country, depending on the form type.

3. Access for CPMS must be submitted through MyAccess.
4. For more information and training on CPMS, see CPMS Connect site.

Chapter 3 - EDMS

1. EDMS (Enterprise Document Management System) is a web-based technology to view, search, and store digitized versions of immigration records.
2. EDMS Receipts contain digitized Receipt files that have been processed by USCIS Office of Intake and Document Production (OIDP) Lockbox Operations.
   a. Lockbox provides document scanning, metadata capture, and creation of information into EDMS.
   b. Images are available approximately 24 hours after intake.
   c. Receipt files are not electronically combined after the Receipt file has been physically combined with an A-file and the A-file has been digitized.
   d. A Receipt file that has associated or related Receipt files will indicate "Show Associated Receipt Files."
3. EDMS A-files contains digitized A-files and T-files
   a. NRC manages the digitization program of A-files and T-files. For more information including interfiling and consolidation of digitized records refer to the NRC Customer Service Guide.
   b. NRC will digitize A-files relating to information requests sent to the SODATEAM.NRC@uscis.dhs.gov email box.
   c. Images are available approximately 8 workdays if it is at the NRC and 15 workdays if the record is at the Lee's Summit FRC.
4. EDMS contains all documents from the physical record in the digitized record, except:
   a. If material cannot be scanned, the EDMS image is annotated by a document indicating "Unscanned Items. One or more of the following is included in the original A-file, but not scanned: newspaper(s), magazine(s), book(s), audio and/or video cassette(s), catalog(s), CD-ROM(s), Sealed Envelopes, Other;"
   b. An office created a T-file because the original A-file was not available or unable to be located; or
   c. If any information or the record is Classified as EDMS has not been approved to process or contain classified information. If you access an EDMS record and determine that it is classified or contains classified documents, contact your local Records Manager and Field Security Manager. See RPM Vol 3, Part C, Chapter 13 for information on classified records.
5. EDMS records contain all parts of a file, so a 5-part file that is missing part 3 will not be scanned and available in EDMS.

6. EDMS and CIS2 will indicate if a digitized file has been consolidated. RAILS will not indicate if digitized files have been consolidated.
7. For more information on digitized records, see
   a. RPM Vol 3, Part A for description,
   b. RPM Vol 3, Part D for local storage of and requests for an EDMS record, and
   c. The CHAP for adjudicating applications and petitions.
8. Printing copies of a file from EDMS
   a. There is nothing that precludes you from printing a copy of the digitized file from EDMS.
   b. Printed copies must be stored in a W-file and destroyed when it is no longer necessary for business. Exact copies of documents printed from EDMS should not be sent to the NRC.
   c. An exception is if a change/remark has been made to the copy or new material/originals have been added to the work folder. A T-file should then be created for this new material and sent to the NRC for scanning as interfiling. See RPM Vol 3, Part B, Chapter 6,
9. Access for EDMS must be requested via MyAccess and training in PALMS or from IIMD's Information Management Training Branch must be completed before access will be granted.
   d. For descriptions of user roles visit https://connect.uscis.dhs.gov/org/IRIS/IIMD/Systems/Systems/Pages/EDMS.aspx
   e. Designation as a Records Administrator is granted by IIMD and the following requirements must be met:
      v. Verification by supervisor as a trained Records Officer or Immigration Officer with records responsibilities;
      vi. Assignment to an FCO having access to restricted areas in CIS2 and RAILS;
      vii. Justification provided in EDMS access request supports one or more of the functions for the role;
      viii. Completion of training for General User and Records Administrator in PALMS or from IIMD's Information Management Training Branch; and
      ix. Acknowledgment that you have read the General Rules, Requirements, Procedures, and Policy for Designation as an EDMS Records Administrator (available within MyAccess).
10. Requestors must provide a copy of the training certificate to their immediate supervisor/approving organization group to confirm completion of training.
11. EDMS users require varying degrees of access to electronic records. There are three distinct roles that may be assigned to an individual, each with different capabilities and functionality.
12. These three roles and their capabilities are:
    a. General User - can perform basic searches, review, and print watermarked individual documents within an electronic file(s).

b. Records Administrator (RA) – capability to perform General User functions. RA's have the ability to export and print the entire A-file, either with or without the watermark or as a copy for certification, and edit the metadata within the file.
   i. The primary function of the Records Administrator is to export an entire A-file(s) for the purpose of printing, producing a copy for certification, or CD creation.
   ii. Metadata will only be edited when it can be verified by other DHS approved systems (for example, CIS2, CLAIMS, etc.).

c. System Administrator (SA) – capability to perform General User and RA functions. Additionally, SAs have the ability to delete electronic records.

13. EDMS technical problems should be reported to the USCIS Service Desk at 1-888-220-5228 or USCIS Service Desk email.

14. Send EDMS feedback, issues, and concerns to edmsfeedback@uscis.dhs.gov.

15. For detailed guidance on how to use EDMS, see the EDMS User Manual.

16. EDMS CDs
    a. Offices may produce CDs of A-files that have been digitized in EDMS. For detailed guidance on the production and use of CDs, see Exporting and Burning A-files onto CDs and Using the Digitized A-file CD.
    b. Any disk containing information from an A-file is considered to be Sensitive Personally Identifiable Information (SPII) and should be handled in accordance with DHS guidelines, including:
       i. Disks should be physically secured when not in use.
       ii. Disks with PII on them should only be shared with people who have permission and/or a need to view them.
    c. A CD creation and destruction log is not mandatory. However, offices may opt to maintain a log in order to ensure proper handling of SPII.
    d. Never place CDs in immigration records. When the CD is no longer required for official business, place the CD in an approved shredder.

17. EDMS guidance
    a. Memorandum Subject: USCBP Field Guidance on Processing Digitized A-Files
    b. HQRAIO, Issuance of the Final EDMS Procedures Manual - June 2008.
    c. Adjudication and/or Processing of Cases When the File Control Office (FCO) Indicates "DIG" or "RDF".

18. Is the digitized file the official Agency record?
    On March 28, 2008, the Associate Director, NSRV, issued a memorandum to Field Leadership, Subject: Use of Digitized A-Files, Interim Guidance. The purpose of the memorandum is to authorize and direct the use of digitized A-files. Please reference the Digitized A-File Interim Guide for additional information. This policy was re-affirmed on October 05, 2018 when IRIS updated the memo Policy Revision - Records Policy Manual (RPM) Part IX-02 Enterprise Document Management System (EDMS) File Requests.

19. Can I save a digitized document or file to my hard drive?
    To view the memorandum on Interim Guidance on Saving A-Files, refer to the following PDF.

Chapter 4 - RAILS

1. RAILS tracks the location of immigration records, physical, digitized, electronic, and hybrid.
2. RAILS Mobile is an app designed for anyone who handles immigration records for use on government iPhones. Users can search, send, request, receive, track, and audit records from anywhere.
3. The Records Manager is responsible for ensuring that the widgets are monitored and reconciled. See Records Dashboard Quick Reference Guide for more information on widgets.
4. Access for RAILS and the Records Manager Dashboard must be submitted through MyAccess.
5. For more information and training on RAILS, see RAILS Connect site.

Chapter 5 - STACKS

1. STACKS is one of the three NARA-approved digital content management system for immigration records. STACKS allows users to view the application, supporting evidence, correspondence, as well as other internal or applicant submitted content that is considered part of the official immigration record and gives users the ability to search, add notes, tag, and filter through content.
2. In the case of eProcessing applications, the electronic documents located in STACKS constitute the ROP. These documents are uploaded by the benefit applicant or created electronically, so there is no paper copy.
    a. The need to scan documents into STACKS should be rare. When a paper document must be scanned into STACKS, for example when the benefit applicant sends documents through the mail rather than through their myUSCIS account, the paper submissions are unofficial, non-record copies.
    b. Any paper documents scanned into STACKS for inclusion with an eProcessing application must be forwarded to the HBG until approved for destruction in accordance with the retention schedule and IRIS policy.
    c. Only paper documents associated with an existing electronic Receipt file or A-file may be scanned into STACKS.
    d. For scanning/uploading guidelines, see IRIS Quality Assurance / Quality Control for Scanning Records.
3. Users can access STACKS through the case management systems (for example, C3, INFACT, Global, ELIS, et cetera) or via the internet at STACKS login.

4. Access for STACKS must be requested via MyAccess and training in PALMS or from IIMD/IMTB must be completed before access will be granted.
5. For more information and training on STACKS visit STACKS Connect site.

Chapter 6 - TRKS (Transaction Record Keeping System)

1. The TRKS (Transaction Record Keeping System) is a subsystem of CIS2. TRKS provides an audit trail of the activities CIS2 on-line and batch users perform, including any additions, deletions, or modifications.
2. Access to the complete TRKS database is limited to Records Supervisors and District Records Managers and must be requested through MyAccess. Non-supervisors may only request access to transaction 7101 (Query Audit Data Screen), which allows the user to specify the parameters for an audit data query.
3. Before requesting access to TRKS, an employee must have CIS2 access and Tier 1 clearance.
   a. Tier 1 clearance is for non-sensitive positions.
   b. To obtain a Tier 1 clearance, complete Form SF-85, Questionnaire for Non-sensitive Positions and submit to the appropriate supervisor.
4. IIMD is the final approver for TRKS access requests and will not grant requests for access until the applicant submits proof of completion of the TRKS training.
5. For more information on TRKS, see TRKS User Manual.

Chapter 7 - Digitization FAQs

1. Does the digitized A-file include all material or do I have to do a search to see if there is other material that exists, that is T-files?
   a. The digitized file in EDMS may not include all material that exists for the A-file. Because offices create T-files (temporary files) to store permanent documentation when the original A-file has been digitized and not available, you will want to do a RAILS search. RAILS has the capability to track multiple T-files for each A-file.
   b. The interfiling folder within the Enterprise Document Management System (EDMS) will contain scanned material received at the NRC which consists of any:
      i. Loose material received at the NRC; or
      ii. Information received and/or contained in a T-file.
   c. For further information on T-files, see RPM Vol 3, Part A, Chapter 2 and RPM Vol 3, Part E, Chapter 2.
2. How do I adjudicate or process a case when the A-file is digitized?

For further information, refer to the procedural guidance supplied in the joint memorandum from USCIS Records and the Transformation Program Office, Subject: Adjudication and/or Processing of Cases When the File Control Office (FCO) Indicates "DIG" or "RDF" , the USCBP Field Guidance on Processing Digitized A-Files, or the HQRAIO, Issuance of the Final EDMS Procedures Manual.

3. How do I request a correction to a digitized file?
   In certain situations, it may be necessary to make a correction to a digitized file. To request a correction to the digitized record, email edmssupport@uscis.dhs.gov. For further information regarding corrections to a digitized file, see RPM Vol 4, Part B, Chapter 3.

4. Is EDMS accessible 24 hours a day, 7 days a week?
   Yes. EDMS is accessible 24 hours a day, 7 days a week. There is scheduled maintenance which usually occurs on the weekends. Users are informed in advance via a Broadcast Message indicating when EDMS will be down.

5. What happens if EDMS is down or if I need information from a digitized file after hours or on a weekend?
   Contact the National Records Center (NRC) Information Liaison Branch (ILB) at 1-816-350-5560. The NRC is available 24 hours a day, 7 days a week (Except Thanksgiving and Christmas).

6. How do I certify a document from a digitized file?
   d. To certify a document from a digitized file, a Records Administrator (RA) will print a non-watermarked copy of the requested document from EDMS and then follow the certification process outlined in the RPM Vol 3, Part F, Chapter 3.
   e. To certify an entire digitized A-file, an RA will perform a "Certified Copy" export using the EDMS export function, print the documents in the file and then follow the certification process outlined in the RPM.
   f. NOTE: Records Administrator's (RA's) have the ability to export and print the entire A-file.

7. Are there plans in place for A-files to be phased out and replaced with digitized A-files? Is this the "wave" of the future?
   USCIS is embarking on an enterprise-wide transformation effort that will transition the Agency from a paper-based filing system to a centralized and consolidated electronic environment. This effort will require re-engineering of agency-wide business processes and updating information technology systems to provide new capabilities to employees and customers. For more information visit the USCIS Connect website.

8. Once a file has been digitized, is the file shipped to the NRC?
   Files are digitized at the NRC and retired to the FRC at a later date.

9. Will overseas offices have access to EDMS?

Yes. If you do not have EDMS access and require it, request access via MyAccess. Requestors must complete the EDMS Orientation training available via PALMS or complete the EDMS training through classroom or webinar from the USCIS Records Academy before access will be granted. Requestors must provide a copy of the training certificate to their immediate supervisor/approving organization group to confirm completion of training.

10. What is the intended use of the digitized Receipt files?
    The digitized Receipt files are images of applications processed by the Lockbox, and are not considered the official Agency record of the Receipt file. The paper file is the official record for the Agency. The Receipt files in EDMS are intended to be used to research customer inquiries on accepted and rejected applications processed by the Lockbox and to begin initial work on an application before the hardcopy is received.

11. When I try to view a document my browser displays a blank page.
    Please contact the DHS Help Desk at 1-888-220-5228 to obtain the necessary software update to resolve this issue.

12. Can I search by a partial date of birth?
    No. Currently the full date of birth is required in order to use date of birth as a search criterion.

13. How does the Basic Search work?
    The Receipt-Number search is an exact match search. Receipt numbers are stored as 13 alphanumeric characters and the users must enter 13 characters when performing a search.

14. How do I edit a Receipt File?
    Editing Receipt files is not allowed in EDMS.

15. When I refresh my browser window I see a blank screen or get an error.
    With the current implementation of EDMS the built-in browser controls are not fully functional. The user should rely on EDMS's navigational elements.

16. When I use the back button on my browser I see a blank screen or get an error.
    With the current implementation of EDMS the built-in browser controls are not fully functional. The user can try refreshing the screen via the browser controls. Alternatively, the user should rely on the navigational elements built in to EDMS.

17. The right button on my mouse does not appear to work in EDMS. Why?
    The right button on a mouse gives the user access to features such as opening a web page in a new browser window or going back in the browser window. Since these features are unavailable in EDMS the option of clicking the right mouse button has also been disabled.

18. When I search for a Receipt file using information about the individual (for example, name), it can't be found. Why?
    The first name, last name, date of birth, and A-number fields are all optional fields for Receipt files and may not be populated. Try searching by Receipt number.

Part C - Reporting Tools and Analytics

Chapter 1 - Standard Management Analysis and Reporting Tool (SMART)

1. The Standard Management Analysis and Reporting Tool (SMART) is a web-based reporting and analytics tool that allows access to many data sets from source USCIS systems, such as C3, C4, ELIS, etcetera.
2. For access, training, and information on SMART, see SMART ECN site.
3. SMART extracts data from multiple USCIS records management systems and organizes and displays this data in pre-built standard dashboards and reports.
4. See Appendix F for a list of SMART reports generated from RAILS data that are required to be reconciled.
5. IIMD uses the following six reports to create an office's Health Score to monitor compliance with records management policy:

SMART Reports Related to Health Score	Frequency
In transit over 60 days	Weekly or more frequently based upon local office requirements
Duplicate files (Pairs)	Quarterly
Match A- and T- files (pairs)	Quarterly
Unaudited empty jackets over 183 days	Required before and after every audit
Unaudited files	Required before and after every audit
Unaudited classified files over 183 days	Required before and after every audit

Chapter 2 - Secure Report Distribution Utility Reports

1. Secure Report Distribution Utility (SRDU) reports give Records Managers a tool to ensure multiple A-numbers are not issued to a single individual and that A-number records are being created and verified in CIS2 for all physical A-files assigned. These reports serve as a daily or monthly reminder to complete certain existing records management functions to ensure data integrity, action is required by your FCO.
2. For access and information on SRDU, see SRDU guide.
3. Users have the ability to access the following three reports:

a. Daily Override Report - identifies all New File Add (9301) and Verify New File Add (9302) records that were manually created in CIS2 using the Override transaction because there were already existing exact matching name/DOB/COB record(s) in CIS2. The Override Report allows Records Managers to view these A-number records so they can follow-up to ensure duplicate A-numbers are not being assigned.
b. Non-Verified New File Add Delinquents Report (daily) - identifies all verification records between 5 and 14 days old that were added to the verification portion of the CIS2 database through a New File Add (9301) transaction but not yet added to the CIS2 database because they are still waiting to be verified with a Verify New File Add (9302) transaction. The Delinquents report allows Records managers to view verification records that have not been verified within the 48-hour time period required by the RPM so they can ensure the records are verified and added to CIS2.
c. Non-Verified New File Add Deletions Report (monthly) – identifies all verification records that were deleted 15 days after they were added to the verification portion of the CIS2 database through a New File Add (9301) transaction. These records were deleted because a Verify New File Add (9302) transaction was not performed within the 14 day timeframe to add them to the CIS2 database. The Deletions Report allows Records Managers to view deleted verification records so they can follow-up with their employees to find out why the record was not verified and added to CIS2, to ensure an A-file was assigned, and a record for the A-number is successfully created in CIS2.

Volume 5 - Reserved

Volume 6 - Continuity of Operations

Part A - Continuity of Operations Planning

Chapter 1 - What is Continuity Planning

1. The Continuity of Operations Planning (COOP) process focuses on keeping the essential functions of an organization operational during crises situations. The process includes writing, testing, and implementation of plans.
2. The primary function of the COOP process is protecting the welfare and safety of our employees and identifying and protecting critical and historical records.
3. Continuity planning applies to anything that would interrupt normal operations. This could be power failures, natural disasters, terrorist activities, etc.
4. The COOP process is not just a single plan, it is an approach that incorporates a variety of plans from every DHS Field Office.
5. The Integrated Emergency/Response Recovery Plans (IERP) is the local single source of information to consult during an incident. It gives the information needed to respond to an incident and refers to any other, more detailed documentation that may be useful. The IERP must be designed:
   a. To protect people;
   b. To prevent avoidable problems;
   c. To protect vital records; and
   d. To react effectively and efficiently in the event of a disaster.
6. See the library of reference that may help with developing local plans, including a sample IERP.

Chapter 2 - Why Have Continuity Planning

1. Protecting records from damage or loss is an essential records management role. Adequate care must be taken to protect and safeguard the Service's records.
2. Service employees will know how to react during a disaster because they will know how to protect themselves, the organizations priorities, and their roles and responsibilities.
3. Continuity planning ensures continuation of operations, improved security and safety, and protection of vital assets like critical records.
4. Loss of critical records can mean loss of rights and benefits for individuals, loss of funds or other assets, and the organization would not be able to carry on normal operations.
5. Critical records are defined by the
   a. Historical value,
   b. Impact of protecting the legal and financial rights of private citizens,

c. Value in documenting land and the environment, and
d. Impact in protecting the legal and financial rights of the government.

6. DHS critical records include but are not be limited to:
   a. A-files;
   b. Receipt files;
   c. Personnel files; and
   d. Investigative files.

Chapter 3 - Continuity Planning Roles and Responsibilities

1. USCIS Headquarters is responsible for developing a COOP for the Service.

2. IIMD is responsible for
   a. Providing tools and articles for use in developing local plans;
   b. Maintaining a service-wide repository of IERPs on the intranet;
   c. Reviewing local plans; and
   d. Conducting testing of local plans.

3. The Region is responsible for
   a. Appointing a main and alternate point of contact who will coordinate recovery responses, which may include arranging for supplies or additional staff;
   b. Providing contact information for the primary and alternate points of contact to IIMD and the Regional offices;
   c. Developing and implementing a regional office IERP;
   d. Providing an electronic copy of each IERP to IIMD;
   e. Maintaining a central library of all IERP for all offices in the Region;
   f. Reviewing local plans for sufficiency and completeness;
   g. Monitoring plan updates; and
   h. Conducting on-site testing at the regional and local offices.

4. Each FCO is responsible for
   a. Creating and maintaining an IERP that covers their office, all FCOs, Sub-offices, Ports of Entry, and Asylum offices within their jurisdiction;
   b. Coordinating the plan with subordinate offices;
   c. Implementing the plan;
   d. Updating the plan on a regular basis; and
   e. Conducting recovery training and on-site testing.

5. Each local plan must take into consideration the needs of the subordinate offices, especially for remotely located offices. This does not preclude a subordinate office from creating a plan.

6. Regional offices must forward the plan to a Regional Records Office.

7. Service Centers must forward the plan to IIMD with an information copy to HQ Service Center Operations.
8. Asylum and Foreign offices must send the plan to IIMD with an information copy to HQ International Affairs.
9. Border Patrol offices must send the plan to IIMD with an information copy to CBP.

Chapter 4 - Records Disaster Action Team

1. Offices should establish a Records Disaster Action Team. This team will:
   a. Develop and implement the local IERP;
   b. Coordinate with your next higher headquarters level; and
   c. Establish a schedule to review and update the plan.
2. The Records Disaster Action Team members should include:
   a. Records Disaster Action Team Coordinator;
   b. Building Manager;
   c. Security Officer;
   d. Health and Safety Liaison;
   e. Administrative Liaison;
   f. Media Relations;
   g. Communications Liaison;
   h. Recovery Operations Coordinator;
   i. Records Officer: Agency Services; and
   j. Computer Systems.

Chapter 5 - Basic Contact Information

1. Your plan, contained in the emergency handbook, needs some basic contact information. With further guidance, you will use this information to provide roles and responsibility information and contacts for specific types of incidents.
2. Create a listing of all personnel to include their:
   a. Home phone number;
   b. Address;
   c. Emergency contact;
   d. Office extension; and
   e. Supervisor name.
3. Include a list of emergency contacts, phones numbers, and points of contact in the emergency handbook. Be sure to include:
   a. Police;
   b. Fire Department;
   c. GSA or facility manager;
   d. The local emergency number and the number for reporting non-emergency incidents;

e. Director;
f. Security Officer;
g. Contact at next higher headquarters level;
h. NARA;
i. FEMA;
j. OSHA;
k. EPA;
l. Public Health; and
m. CDC.

Chapter 6 - Facility Assessment

1. Each location should conduct quarterly inspections of their location. These inspections will identify potential hazards, deficiencies, and exits.
2. If you are located in a leased facility you must coordinate your efforts with the landlord's facility manager and/or building supervisor.
3. The reference material contains a form that you can use to help develop a local Facility Assessment Form.
4. Inspect areas to ensure ceiling tiles are secure and free of water damage.

Chapter 7 - Supply Maintenance

1. Each office/location will keep on hand materials to handle simple disasters or emergencies. The material contains a generic list of the type of material needed.
2. It is best to disperse these items throughout the facility so they will be close at hand. Plastic tubs are a good choice for storing the items.
3. Inventory disaster supplies quarterly.

Chapter 8 - Preventing Damage

1. To mitigate damage ensure employees are properly trained and know what to do before an incident occurs.
2. Ensure emergency handbooks are available to managers and supervisors both on- and off-site, in electronic and paper format, and contain (at a minimum):
   a. Contact information;
   b. Facilities Assessment;
   c. The location and description of vital records;
   d. Reference material on recovery techniques for paper records; and
   e. Contact information for local vendors.
3. At a minimum, make sure your employees know where to report in case of an emergency. To prevent fire damage, each office must

a. Enforce all existing local fire regulations with respect to doors, extinguishers, sprinkler systems, and alarms;
b. Inspect the expiration date of all fire extinguishers;
c. Maintain a list of flammable substances and isolate them;
d. Maintain Material Safety Data Sheets (MSDS) for each substance in the emergency handbook;
e. Keep storage areas neat and clean;
f. Ensure that file rooms are not cluttered; and
g. Schedule regular inspections to ensure appropriate maintenance of fire and safety equipment.

4. To prevent water damage, each office must
   a. Identify and visually inspect on a regular basis potential internal and external hazards (for example, sprinkler systems, water pipes, HVAC systems, windows, and doors) for leaks and cracks;
   b. Consider installing water monitors/alarms in below-grade rooms/basements;
   c. Raise bottom storage shelves a minimum of two inches above the floor. Kick plates are recommended; and
   d. Not store records on the floor whether in folders or boxes.
5. To prevent insect and rodent infestations:
   a. Do not eat or drink in the stacks;
   b. Avoid storing food in the stacks; and
   c. Inspect regularly for insects and vermin.
6. To prevent computer damage and/or damage to electronic information, work with the Incident Response Manager (IRM) on computer security and contingency plans.

Part B - National Security Events

Chapter 1 - Determination of an NSE

1. A National Security Event (NSE) is any situation that involves potential or actual terrorist acts or terrorist threats, where such acts are within the federal criminal jurisdiction of the United States and require the Federal Bureau of Investigation (FBI) Joint Terrorist Task Force (JTTF) to coordinate the activities of the other members of the law enforcement community.
2. ICE determines when an NSE occurs.
3. In consultation with the Director of USCIS and USCIS' Fraud Detection and National Security (FDNS) Associate Director, ICE's Homeland Security Investigations (HSI) Assistant Director or designee makes a request to the FDNS Associate Director to invoke the procedures of RPM Vol 6, Part B.

4. When an NSE designation is made, HSI will provide to FDNS an HSI Point of Contact (POC) who will be responsible for the receipt of the copy of the immigration record.
5. ICE HSI assumes its DHS-designated role as the lead agency for the dissemination of information that is contained within immigration records (electronic or paper copies of physical immigration records) to the JTTF, other law enforcement agencies, and the intelligence community. HSI will designate POC within every Special Agent in Charge (SAC) office and will work with the local FDNS offices to implement procedures consistent with this policy.
6. Incidents covered under this Part are time critical and must be given work priority status to ensure necessary actions are taken in a timely manner to facilitate law enforcement investigative needs.
7. When the provisions of this Part have been invoked, USCIS and FDNS must refer all requests for information or documentation from the immigration record(s) made by other law enforcement agencies or the intelligence community to the HSI POC. The HSI POC will respond to the requests as appropriate.
8. Access to and sharing of immigration records in accordance with this Part will be coordinated with FDNS and the USCIS Records Supervisor in the office(s) where the record(s) are located.
9. FDNS will notify local USCIS leadership and the local FDNS supervisor regarding immigration record(s) in relevant office(s)/area(s) that are needed to address the NSE. If the FDNS supervisor is not located at an FCO, a designated local FDNS immigration officer will be responsible for coordination of record movement. FDNS will provide the local FDNS POC with the name and contact number of the HSI POC for receipt of immigration record information.
10. Other than digitized records at an FRC, this Part does not apply to situations in which the record is in electronic form and accessible to ICE via EDMS.
11. If the requested records are classified, the FCO that has custody of the record must verify that the recipient has appropriate clearance and or a courier card, see RPM Vol 3, Part C, Chapter 13.
12. If, during the NSE, an administrative or criminal arrest is made of an individual associated to the event, the original immigration record must be sent to the local HSI office where the administrative or criminal violations are being prosecuted.

Chapter 2 - Immigration Records Located at a USCIS FCO

1. Within 2 hours of receipt of the record, the local FCO's Records Supervisor must provide a hard copy and an electronic copy of the immigration record(s) to his or her local FDNS POC.

2. Per the discretion of FDNS, the NRC may provide copies directly to HSI. If copies are provided directly to ICE, the NRC must assume all duties of a local FDNS POC in consultation with the NBC FDNS POC.
3. Within 30 minutes of receipt of the record copy, the local FDNS POC must provide a hard copy and an electronic copy of the immigration record to the HSI POC.
4. The FCO Records Supervisor must update the record location in RAILS and initiate a record hold by:
   a. Updating the location to the Responsible Party Code (RPC) of the local FDNS supervisor;
   b. Placing the record on hold (In-Use) for one year, see RPM Vol 6, Part B, Chapter 7 for guidance on extensions; and
   c. Entering a note in the comment field indicating the hold date and the hold expiration.
5. The FCO must sequester/secure the hard copy record and not honor any record requests without coordinating with FDNS.
6. FDNS must refer all inquiries for information or documentation to the HSI POC.

Chapter 3 - Retired Immigration Records

1. The NRC must make an expedited request for a retired record from the FRC.
2. Immediately upon receipt, the NRC must provide a hard copy and an electronic copy of the records to the NBC FDNS POC.
3. Per the discretion of FDNS, the NRC may provide copies directly to HSI. If copies are provided directly to HSI, the NRC must assume all duties of a local FDNS POC in consultation with the NBC FDNS POC.
4. Within 60 minutes of receipt of the record, the NBC FDNS POC will provide a hard copy and electronic copy of the record to the ICE HSI POC.
5. The NRC must then follow the sequestration protocols in RPM Vol 6, Part B, Chapter 7.

Chapter 4 - Immigration Records Located at an ICE Office (including ICE FCOs)

1. This Chapter does not apply to immigration records belonging to subjects in administrative or criminal proceedings. See to RPM Vol 6, Part B, Chapter 5 for guidance on immigration records for aliens in proceedings.
2. The local USCIS FCO must complete the following steps in order to retrieve an immigration record located at an ICE office:
   a. Request the physical record from the ICE office where the record is currently located;
   b. Alert the ICE Headquarters Liaison, the Records Branch within the ICE Privacy and Records Office, by email that an immigration record retrieval request under this Part has been issued to the ICE office where the physical record is currently located.

iii. Send email to FileNationalSecurityEvent@ice.dhs.gov, accessible to Records Branch personnel after normal business hours;
iv. The subject line of the email should read "National Security Event Request;"
v. The A-number and the ICE office that has custody of the record must be included;
vi. The ICE office that holds the record must return it to the requesting FCO;
vii. In the event the FCO has difficulty obtaining the record from the ICE office in a timely manner, the ICE Records Branch will facilitate the request and ensure the record is provided to the FCO.

c. Retrieve the record from the ICE office. The local ICE office will make a hard copy of the record before it leaves ICE's custody. The record(s) must be hand-carried back to the FCO. If the ICE office is more than ten miles away, the FCO must consult with the FDNS POC in order to determine the most efficient method of acquiring the record or the record's content.

3. Within 2 hours of receipt into the FCO, the local FCO's Records Supervisor must provide a hard copy and an electronic copy of the record to the local FDNS POC.

4. Within 60 minutes of receipt of the record copy from the FCO, the local FDNS POC will provide an electronic copy of the record to the HSI POC.

5. After providing a record copy to the FDNS POC, the local FCO must follow the sequestration protocols in RPM Vol 6, Part B, Chapter 7.

Chapter 5 - Immigration Records for Aliens in Proceedings

1. If the person of interest is involved in an ICE administrative or criminal proceeding, the local FCO must request a hard copy and an electronic copy of the immigration record by sending an email to A-FileNationalSecurityEvent@ice.dhs.gov.
   a. The subject line of the email should read "National Security Event Request;" and
   b. The A-number and ICE office that has custody of the record must be included.

2. The local FCO will make a hard copy and an electronic copy of the record at the ICE office that has custody of the record.
   a. The electronic copy must be in a single .pdf file.
   b. The record copies must be hand-carried back to the local FCO.
   c. If the ICE office is more than ten miles away, the FCO must consult with the FDNS POC in order to determine the most efficient method of acquiring the immigration record content.

3. Within 60 minutes of receipt into the FCO, the local FCO's Records Supervisor must provide a hard copy and an electronic copy of the record to the local FDNS POC.

4. The FCO must secure the hard copy and electronic copies of the record.

5. FDNS must refer all inquiries for information or documentation to the HSI POC.

Chapter 6 - Digitized Immigration Records

1. If an immigration record has already been digitized and the physical record is located at an FRC, FDNS will provide the NRC with guidance regarding level of control appropriate for the record(s).
2. Until otherwise directed, the EDMS level of control will be "OPEN".

Chapter 7 - Releasing Holds on Immigration Records

1. Records that are within the initial 1-year hold period may be released per guidance from ICE. The local FDNS supervisor is responsible for notifying the appropriate FCO when the record may be released for normal processing.
2. ICE and/or FDNS must request an extension of the initial 1-year hold period by notifying the local FDNS supervisor.
   a. The FDNS supervisor will notify the appropriate FCO regarding the extension.
   b. The FCO will place the record on hold in RAILS for subsequent 6-month periods while any related investigations are ongoing.
   c. The FCO will note the updated expiration date in the comment field.
   d. Subsequent extension requests may be submitted pursuant to this section following the hold expiration date.
3. If a sequestered record is requested and the hold expiration date has passed,
   a. The FCO must notify the local FDNS supervisor of the record request; and
   b. The local FDNS supervisor must request a release of the record from the HSI POC. If the record cannot be released, HSI and/or FDNS must request an extension of the hold.

Part C - Furloughs

Chapter 1 - General

1. A furlough occurs when there is a lapse in appropriations or upon expiration of a continuing resolution, if a new continuing resolution or appropriations law is not passed.
2. In a shutdown furlough, an affected agency must shut down any activities funded by annual appropriations that are not excepted by law.
3. Some agency functions have alternative funding sources and, as a result, are not directly affected by a lapse in annual appropriations. Employees performing these functions continue to work through a furlough.
4. For additional furlough guidance, see U.S. Office of Personnel Management (OPM) website.
5. When Agencies are notified of an impending shutdown/furlough, they must have procedures in place to ensure accessibility of immigration records to ensure all records are accurately reflected in RAILS.

Chapter 2 - Working through a Government Shutdown/Furlough

When Agencies are notified of an impending shutdown/furlough, they must have procedures in place to ensure file accessibility during the shutdown/furlough and ensure all files are accurately reflected in RAILS.

Appendix A - Acronyms

Acronym	Description
AAO	Administrative Appeals Office of USCIS
ARCIS	Archives and Records Centers Information System
ASC	Application Support Center
ASC-ISO	Application Support Center Immigration Services Officer
ASCM	Application Support Center Manager
BCC	Border Crossing Card
BCU	Background Check Unit
BOIB	Business Operations and Integration Branch of IIMD
CFR	Code of Federal Regulations
CBP	U.S. Customs and Border Protection
CCD	DOS's Consular Consolidated Database
CHAP	Consolidated Handbook of Adjudication Procedures
CIS2	Central Index System
CLAIMS	Computer-Linked Applications Information Management System
COB	Country of Birth
COC	Country of Citizenship
CPMS	Customer Profile Management System
DHS	Department of Homeland Security
DIGB	Data and Information Governance Branch of IIMD
DOB	Date of Birth
DOJ	Department of Justice
DOS	Department of State
EAD	Employment Authorization Document
EARM	ENFORCE Alien Removal Module
EDMS	Enterprise Document Management System
EOIR	Executive Office for Immigration Review of DOJ
EPS	Egregious Public Safety
FBI	Federal Bureau of Investigation
FCO	File Control Office
FDNS	Fraud Detection and National Security Directorate of USCIS
FDNS-DS	Fraud Detection and National Security Data System
FEMA	Federal Emergency Management Agency
FOD	Field Office Directorate of USCIS
FOIA/PA	Freedom of Information Act / Privacy Act
FOUO	For Official Use Only
FPS	Federal Protective Service

Acronym	Description
FRC	Federal Records Center
FSM	Field Security Manager
FTR	File Transfer Request
HQ	Headquarters
HSDN	Homeland Security Data Network
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometrics Identification System
IdHS	Identity History Summary
IIISB	International and Interagency Information Sharing Branch of IIMD
IIMD	Identity and Information Management Division of IRIS
IJ	Immigration Judge
IMTB	Information Management Training Branch of IIMD
INA	Immigration and Naturalization Act
IRAD	International and Refugee Affairs Division (formerly RAD)
IRIS	Immigration Records and Identity Services Directorate of USCIS
LHM	Letterhead Memorandum
LPR	Lawful Permanent Resident
LSO	Local Security Officer
MFAS	Marriage Fraud Amendment System
MIDAS	Microfilm Index Digitization Application System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NaBISCOP	National Background Identity and Security Checks Operating Procedures
NAILS	National Automated Immigration Lookout System
NARA	National Archives and Records Administration
NASS	National Apointment Scheduling System
NBC	National Benefits Center of FOD
NCIC	FBI National Crime Information Center
NCIC-II	National Crime Information Center Interstate Identification Index
NGI	Next Generation Identification (formerly known as IAFIS)
NIIS	Nonimmigrant Information System
NLETS	National Law Enforcement Telecommunications System
NQP	Naturalization Quality Procedures
NRC	National Records Center Directorate of IRIS
NTA	Form I-862 Notice to Appear
OSI	Office of Security and Integrity
PAB	Policy Analysis Branch of IIMD
PCQS	Person-Centered Query System

Acronym	Description
PII	Personally Identifiable Information
RAFACS	Receipt and Alien File Accountability and Control System
RAIO	Refugee, Asylum and International Operations Directorate of USCIS
RAP	Record of Arrest and Prosecution now known as IdHS
RAPS	Refugees, Asylum, and Parole System
RFE	Request for Evidence
ROIT	Record of Inquiry – TECS
ROP	Record of Proceeding
RPC	Responsible Party Code (in RAILS)
RPM	Records Policy Manual
SCOPS	Service Center Operations Directorate of USCIS
SEVIS	Student and Exchange Visitor Information System
SIMB	Systems Integration and Modernization Branch of IIMD
SIR	Significant Incident Report
SODA	Scan On Demand Applications
SOF	Statement of Findings
SOP	Standard Operating Procedures
SORN	System of Records Notices
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
TECS	(formerly) Treasury Enforcement Communications System
TIDE	Terrorist Identities Datamart Environment
TPS	Temporary Protected Status
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
U.S.	United States
USC	United States Code
USCG	United States Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	United States Secret Service
VAWA	Violence Against Women Act
WFC	Western Forms Center
WRAPS	DOS's Worldwide Refugee Admissions Processing System

Appendix B - Updating Records for Deceased Subjects

Record Location	Action
Your FCO; San Bruno FRC – retired by your FCO; or FRC Classified Records – retired by your FCO	Request the record and continue the update process
Another FCO or FRC - retired by another FCO	Send the death certificate to the Records Unit of the FCO with the file. Include a routing slip with the A-number.
NRC	Send the death certificate to the NRC in a separate envelope: NRC 150 Space Center Loop Suite 700 Lee's Summit, MO 64064-2141
FRC - retired by your FCO	Complete an Interfile Request routing sheet – Federal Records Center and send with the death certificate in a separate envelope to the NRC using address above. This is ONLY for death certificates.
No A-file, there is a C-file or other historic file	Send death certificate to IIMD. Include a routing slip with the A-number.
No physical A-file, only an electronic record for EAD cards, border crossers, and other non-benefit related A-numbers. (Excluding ELIS records).	You must be able to definitively link the death certificate to the A-number with a DHS-issued identity card. For example, someone may turn in an EAD card with a death certificate. In such cases, as they do not relate to a benefit or immigration action that is tracked via physical documentation, do not create a record.
Lost	Start the lost record process. If you can definitively link the death certificate to the A-number with a DHS-issued identity card, create a T-file. If not, follow the directions for when A-files cannot be located.

Appendix C - Requesting Historical Records

Record Number	File Series	Period Covered	How To Obtain	Send Request To
C-1268430	Certificate files	Sept 27, 1906-Mar 31, 1956	ORM Request if file is 6,500,000 and below OR date of naturalization/issuance is before April 1, 1956	IIMD
DA-64732 AA-3462 A-54987	Derivative Certificate files	1929-1956		
OS-12765	Overseas Military (Korean War) Certificate files	1950-1956		
OM-34987	Overseas Military (World War II) Certificate F-files	1942-1946		
OL-56467	Old Law Certificate files	1929-1956		
B-615	B Certificates of Repatriation	1918-Jan 1, 1941		
D-960	D Certificates of Repatriation	Jan 13, 1941 – (1956?)		
CO 235	CO Subject files	Apr 1, 1957 – Sept 30, 1995	ORM Request if file is 6,500,000 and below OR date of naturalization/issuance is before April 1, 1956	IIMD
56242/849	Old Series Subject Correspondence files	1906 – Mar 31, 1957	All files transferred to NARA	Contact NARA Civil Reference Supervisor at (202) 501-5395
3061123 62551	Visa files	Entries Jul 1, 1924 – Mar 31, 1944	ORM Request	IIMD
CR-653 CR-198548	Certificate of Registry	1929-1944	Request Manual Index name search to obtain Registry File number	IIMD
R-3598 R-216873	Registry file	1929-1944	ORM Request	IIMD

Record Number	File Series	Period Covered	How To Obtain	Send Request To
A 2 453 876	AR Prints	Aug 1940 – Mar 1944	ORM Request	IIMD
A11 684 546	A-files	Jan 1941-1975	ORM Request	FCO holding file, if known; IIMD if not known
A45 684 546	A-files	1975 – present	CIS2	FCO holding file
V-68534	Nonimmigrant V-File, file number taken from FS 257	1951-Jan 1955	ORM Request	FRC
T-63842	Nonimmigrant T-File, file number taken from I-94	1951-Jan 1955		
E-65432	Warrant or Expulsion E-File, file number taken from I-154	1951-1952		

Appendix D - Closed Receipt Files to Send to the HBG

Form	Title	Notes
I-90	Application to Replace Alien Registration Card	Approvals and denials when adjudicated via paper
I-102	Application for Replacement/Initial Nonimmigrant arrival Departure Document	Approvals only for Students and Non-students
I-129	Petition for a Nonimmigrant Worker	Approvals and denials
I-129S	Nonimmigrant Petition Based on Blanket L Petition	Approvals and denials
I-131	Application for Travel Document	Approvals and denials
I-539	Application to Extend/Change Nonimmigrant Status/F-1 or M-1 Student Reinstatement	Approvals and denials
I-765	Application for Employment Authorization	Approvals and denials for all forms except initial I-765s concurrently filed with the I-821 (TPS) and I-821D (DACA) applications
I-824	Application for Action on an Approved Application or Petition	Approvals and denials
I-865	Sponsor's Notice of Change of Address	
N-565	Application for Replacement Naturalization/Citizenship Document	Approvals and denials
	All applications/petitions with returned checks	

Appendix E - Closed A-files to Send to the NRC

Form	Title	Notes
I-90	Application to Replace Alien Registration Card	Approvals and denials when adjudicated via paper. ELIS adjudications are destroyed by the Lockbox
I-102	Application for Replacement/Initial Nonimmigrant Arrival Departure Document	Student and non-student denials
I-129F	Petition for Alien Fiancé(e)	Approvals and denials
I-130	Petition for Alien Relative	Approvals and denials
I-140	Immigrant Petition for Alien Worker	Approvals and denials
I-181	Memorandum of Creation of Record for Lawful Permanent Residence	
I-191	Application for Advance Permission to Return to Unrelinquished Domicile	Approvals and denials
I-192	Application for Advance Permission to Enter as Non-Immigrant	Approvals and denials
I-193	Application for Waiver of Passport/Visa	Approvals and denials
I-212	Application for Permission to Reapply for Admission into United States after Deportation or Removal	Approvals and denials
I-213	Record of Apprehension or Interview	If the form has not triggered an A-file creation, send it to TSC for data entry in IBR and set for destruction after 60 days.
I-290/I-290B	Notice of Appeal to the AAU	Approvals and denials
I-360	Petition for Amerasian, Widow(er), or Special Immigrant	Approvals and denials
I-485	Application for Permanent Residence Status	Approvals and denials
I-512	Authorization for Parole of an Alien into the U.S.	
I-526	Immigrant Petition for Alien Entrepreneur	Approvals and denials
I-589	Application for Asylum and Withholding of Removal	Approvals and denials
I-601	Application for Waiver of Grounds of Excludability	Approvals and denials

Form	Title	Notes
I-612	Application for Waiver of the Foreign Residence Requirement of Section 212(e) of the INA, as amended	Approvals and denials
I-765	Application for Employment Authorization	Approvals and denials except for initial I-765s concurrently filed with the I-821 (TPS) or I-821D (DACA)
I-817	Application for Voluntary Departure under the Family Unity Program	Approvals and denials
I-821	Application for Temporary Protected Status	Approvals and denials
I-821D	Consideration for Deferred Action for Childhood Arrivals	Approvals and denials
I-864	Affidavit of Support Under Section 213A of the Act	Interfile with I-130 and I-485. Remains with I-130 and I-485 in the A-file.
I-881	Application for Suspension of Deportation or Special Rule Cancellation of Removal	Approvals and denials

Appendix F - SMART Reports generated from RAILS data

SMART Reports generated from RAILS data	Frequency
External Pending Files Request Report	Monthly
Internal Pending Files Request Report	Monthly
OF-11 Pending Requests Report	Monthly
Outstanding/Pending File Requests Report	Monthly
Transaction by User ID Report	Quarterly
Transaction Completed Report	Quarterly
Matching A, S, T & W Files Report	Quarterly
Retired Files with Active Duplicate Report	Quarterly
Retired Files with Retired Duplicate Report	Quarterly
FRC File Listing by Accession Report	After retirements and as needed or desired
Aged File Holdings Summary Report	As needed or desired
File Listing by Prefix Report	As needed or desired
File Listing by Rider Status Report	As needed or desired
File Listing by Section or RPC Report	As needed or desired
File Listing by Status Code Report	As needed or desired
Office Transfer Out Report	As needed or desired
Files Summary Report	As needed or desired
Deleted Files by User Report	As needed or desired
File Listing by Comment Report	As needed or desired
File Listing by Million Series Report	As needed or desired
Potential Retirement Report	As needed or desired
Transfer In by Office Report	As needed or desired
List of Responsible Party Codes Report	As needed or desired
List of Sections Report	As needed or desired
OF-11 Request Summary Report	As needed or desired
Office Description	As needed or desired
Riding Files by Parent File Location Report	As needed or desired
Riding Files by Child File Location Report	As needed or desired
Sub-File Count Report	As needed or desired