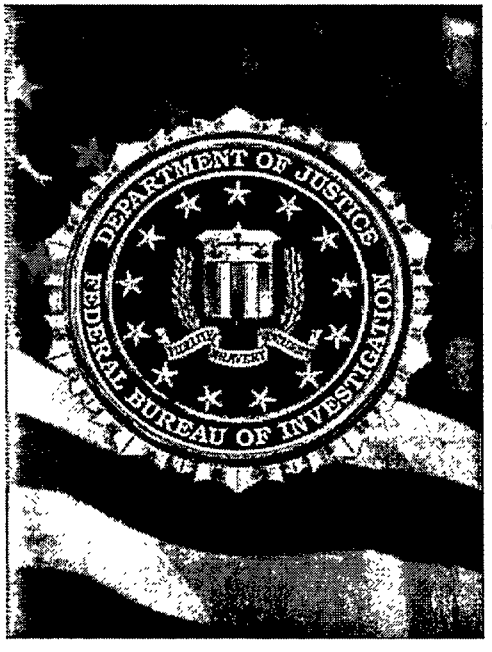
(2)

SENSITIVE

Records Management (RM) Manual



Federal Bureau of Investigation (FBI)

POL05-0001-RMD

Revised August 24, 2007

GENERAL INFORMATION: Questions or comments pertaining to this manual can be directed to:

HQ FBI /Records Management Division, Division 17

William L. Hooton, Assistant Director

Records Policy and Administration Section, Policy and Procedures Unit

[redacted] Chief, Records Policy and Administration Section

[redacted] Chief, Policy and Procedures Unit

b6
b7C

(NOTE: Document is a new publication; no previous versions available.)

PRIVILEGED INFORMATION:

Any use of this report, including direct quotes or identifiable paraphrasing, will be marked with the following statement:

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

FOR OFFICIAL FBI INTERNAL USE ONLY—DO NOT DISSEMINATE

SENSITIVE

Table of Contents

List of Appendices

List of Figures

List of Tables

1. Scope

1.1. Manual Overview

The Records Management manual defines the policies and procedures of the Bureau's records management program, delineates responsibilities for records management, implements Federal records management statutes and regulations, and establishes and communicates standard procedures for the management of FBI records.

1.2. Purpose of FBI Records

The creation and maintenance of authentic, reliable, and trustworthy records is a critical component of every Bureau responsibility and function. Without complete and accessible records, the Bureau cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, or perform any of its critical missions effectively. Deficiencies in the management of Bureau records damage the Bureau's ability to carry out its essential functions and result in inquiries and investigations by oversight bodies as well as adverse public perceptions of the Bureau's efficiency and management.

The FBI is committed to ensuring that its records management program accomplishes the following goals:

- Facilitates the documentation of official decisions, policies, activities, and transactions
- Facilitates the timely retrieval of needed information
- Ensures continuity of Bureau business
- Controls the creation and growth of Bureau records
- Reduces operating costs by managing records according to Bureau business needs and by disposing of unneeded records in a timely manner
- Improves efficiency and productivity through effective records storage and retrieval methods
- Ensures compliance with applicable laws and regulations
- Safeguards the Bureau's mission-critical information
- Preserves the Bureau's corporate memory and history
- Implements records management technologies to support all of the goals listed above

1.3. Benefits of Good Recordkeeping

Adequate and proper documentation provides the information necessary to protect the legal and financial rights of the Federal government, the Bureau, and of persons directly affected by the Bureau's activities; ensures the accountability of the Bureau to the President, the Congress, and the American people; promotes cost-savings in the storage and retrieval of information; and supports the administration of justice and effective law enforcement throughout the Bureau's worldwide operations.

1.4. Federal Records Definition

Federal records are broadly defined to include all recorded information, regardless of medium or format (paper, electronic, audiovisual, etc.), made or received by a Federal agency or its agents under Federal law or in connection with the transaction of public business, and either preserved or appropriate for preservation because of its administrative, legal, fiscal, or informational value.

The Federal Records Act of 1950, as amended, requires all Federal agencies to make and preserve records containing adequate and proper documentation of its organizations, functions, policies, procedures, and essential transactions. Federal records, as defined under the Presidential Libraries Act of 1955 (the Act), are public property and must be managed in accordance with applicable laws and regulations. FBI records may not be destroyed without the approval of the National Archives and Records Administration (NARA).

1.5. Intended Audience

Since all Bureau personnel participate in the creation, maintenance, and use of Bureau records, it is critical that all employees understand Federal records policies and procedures and their own records management responsibilities. Records created or received by employees, contractors, or others serving in effect as Bureau employees (detailees, task force members, etc.) are the property of the FBI—not the creator or recipient of the records. Penalties for the unauthorized destruction, removal, or private use of official records are contained in 18 U.S.C. § 2071 and include fines and imprisonment.

2. Roles and Functional Responsibilities

The assignment of roles and responsibilities for records management is, by statute, a mandatory part of every Federal records management program. Within the Bureau, the roles and responsibilities for records management are as follows:

2.1. The FBI Director:

- Establishes and oversees a records management program for the FBI.
- Delegates responsibilities for managing the FBI's records management program (66-HQ-A1358157-32, 04/29/2002).
- Provides, through annual budget requests to the Congress and other sources, adequate resources for the accomplishment of the FBI's records management program.

2.2. Records Management Division

2.2.1. The Assistant Director:

- Establishes and oversees a comprehensive Bureau-wide records management program.
- Ensures that all divisions are informed of and trained in their responsibilities related to the creation and maintenance of Bureau records.
- Develops and maintains a network of records management liaisons in all divisions and offices and ensures that they receive adequate training to carry out their responsibilities.
- Oversees the management of FBI records throughout their life cycle, to include records creation, maintenance and use, and disposition of recorded information in all media.
- Serves as the Records Officer for the Bureau.
- Oversees the operations of the subordinate sections of Records Management Division (RMD)

2.2.2. The Records Policy and Administration Section (RPAS):

- Establishes and disseminates policies and procedures governing the creation, organization, maintenance, use, preservation, disposition and transfer of all FBI records in all mediums and formats—including paper, audiovisual, cartographic, etc.
- Provides records management training and guidance to all divisions, offices, groups, and organizations throughout the Bureau.
- Conducts periodic audits or evaluations of FBI records programs.
- Manages and regularly updates the FBI Records Retention Plan, coordinating requests for and receipt of all disposition authorities with NARA.
- Oversees the storage of records in offsite storage facilities and the transfer of permanent records to NARA.

- Provides guidance on records policy and disposition aspects of the FBI information technology systems, in coordination with the technical review provided by RMD's Records Automation Section.
- Provides retrieval services for Bureau files in FBI headquarters (HQ) offsite storage locations.
- Resolves problems and provides guidance on recordkeeping policies associated with the Bureau's central filing systems, including the Automated Case Support System.

2.2.3. The Records Automation Section (RAS):

- Develops policy and guidance for the management of records in electronic media. Policy and guidance are coordinated with RPAS to ensure consistency across media.
- Provides document conversion services (both imaging and optical character recognition) through the Document Conversion Laboratory.
- Conducts electronic recordkeeping certification reviews of all information systems.
- Works with the Office of the Chief Information Officer (OCIO) and RPAS to plan and deploy a policy compliant records management application as part of the Bureau's enterprise architecture.
- Plans and assists with the development of an enterprise Records Management Application in coordination with information technology divisions, offices, and groups.

2.2.4. The Records/Information Dissemination Section (RIDS):

- Plans, develops, directs and manages responses to requests for access to FBI records and information, in accordance with the requirements of the Freedom of Information Act and Privacy Act (Title 5, USC, § 552 & 552a), Executive Order 12958, and other applicable Presidential, Attorney General, and FBI policies and procedures as well as judicial decisions).
- Assists the Office of General Counsel (OGC) in requesting and collecting relevant records for certain major criminal investigations, as approved by RMD and OGC.

2.2.5. The National Name Check Program Section (NNCPS):

- Plans, develops, directs and manages responses to requests for access to FBI records and information in accordance with the requirements of the National Name Check Program (Executive Order 10450).

2.3. All Divisions/Offices

2.3.1. The Assistant Director (AD), Supervisory Agent in Charge (SAC), or Assistant Director in Charge (ADIC):

- Appoints a records management liaison to assist RMD in the development and implementation of records management policies and procedures.
- Ensures that the division/office complies with RMD policies by creating and maintaining adequate and proper documentation of all official programs and activities.

- Provides adequate resources and training to enable division/office personnel to participate in and complete records management requirements.

2.3.2. The Records Management Liaison:

- Represents a division/office in coordinating with RMD on all records management policies, procedures, and programs.
- Understands professional records management concepts and Federal records management laws and regulations, through the completion of training provided by RMD and other sources.
- Reviews proposed records management policies within a division/office, providing coordinated review responses to RMD.
- Oversees the creation and maintenance of records in a division/office, advises other employees on FBI recordkeeping requirements.
- Monitors file destruction, file transfer, and litigation freeze activities in compliance with FBI policies and in coordination with RMD's Records Disposition Unit.
- Provides training to others on records management policies and procedures.
- Assists with processing of FOIA and Name Check requests, as necessary, with the resolution of issues involving field division files, in coordination with RIDS and NNCPS.
- Conducts periodic records inventories and records audits, in coordination with RMD's Records Compliance Unit (RCU).

2.4. The Inspection Division

- Includes audits of records management compliance in all FBI division/office inspections using checklists and interrogatories provided by RMD
- Coordinates with RMD's RCU to conduct specialized records audits as appropriate.

2.5. System Administrators

- Ensure that systems are certified for electronic recordkeeping and that all documentation is accurate, available, and legible to personnel when required.

2.6. All Employees

- Create and maintain complete and accurate documentation of all FBI programs, activities, decisions, and transactions.
- Ensure that records are filed appropriately, either in division or Bureau-wide recordkeeping systems such as the Automated Case Support (ACS) system.
- Cooperate with office and division records management liaisons in the creation, maintenance, and disposition of FBI records.
- Ensure that all deletion, destruction, or removal of FBI records is accomplished only in compliance with RMD Records Disposition Unit policies and procedures

3. Policies

Records management policies can be broken down by the main components of the records' life cycle as follows:

- Creation and receipt
- Maintenance and use
- Disposition (destruction or transfer)

3.1. Records Creation and Receipt

Every FBI employee, division, and office has the responsibility to document all activities, decisions, policies, and transactions conducted in accordance with FBI functions and duties.

Documentary materials created in accordance with this responsibility are FBI records. In addition, all documents, databases, and other information received by the FBI in the course of its routine duties and responsibilities are FBI records as well, even though these records were created by other individuals or organizations.

Documents, electronic records, and other information or property received or seized by the FBI or its law enforcement partners, in the course of the investigation of a particular case, may be treated as evidentiary property, not records, and managed under a different set of rules and regulations than those defined in this manual. The chain of custody form (FD 1004) documenting the management of evidence is, however, a record.

See Procedures and Processes: 1.1. What Is a Record?, for records terminology definitions as well as a detailed explanation of what is and isn't a record.

3.1.1. Recordkeeping Requirements Policy

By Federal regulation (36 CFR § 1220), each agency must develop and implement "agency-wide programs to identify, develop, issue, and periodically review recordkeeping requirements for records for all agency activities at all levels and locations in all media." Recordkeeping requirements provide the regulatory means to implement adequate and proper documentation requirements.

It is the responsibility of each Headquarters Division or Office, with assistance from the Records Management Division, to incorporate applicable laws, regulations, or other requirements pertinent to the organization's program responsibilities into recordkeeping requirements for the documentation of their programs.

3.1.2. Recordkeeping Requirements Definition

Recordkeeping requirements are specific instructions, developed by subject-matter experts, for the collection of information or the maintenance of documents for a particular FBI function or program. For example, the rules on what type of data and formatting should be included in an Intelligence Information Report (IIR) are recordkeeping requirements (see IIR Handbook).

Recordkeeping requirements can range from broad, government-wide guidance found in statutes and regulations to office-specific instructions on the preparation of a certain report. What these have in common, however, is that both provide mandatory instructions that tell appropriate agency staff what records to create and how they should be managed. Recordkeeping requirements that simply require the creation and maintenance of a certain type of information are often found in the United States Code, the Code of Federal Regulations, Presidential Directives, or Acts of Congress. These high-level directives may specify recordkeeping responsibilities for particular departments or agencies, but do not usually contain detailed instructions.

Recordkeeping requirements specific to types or classification numbers of records are typically derived from legislation governing the FBI's program areas. For example, The Brady Handgun Violence Prevention Act of 1993 (Brady Act) mandated the establishment of the National Instant Criminal Background Check System (NICS), a system of records maintained by FBI's Criminal Justice Information Services (CJIS) Division. The Brady Act contains instructions on the types of information to be maintained in NICS.

See Procedures and Processes 4.3.1. Which Recordkeeping Requirements Are My Office's Responsibility?

3.2. Records Maintenance and Use

3.2.1. Records Standards

In the records maintenance and use phase of the records life cycle, authentic, reliable, and trustworthy records are readily available (useable) for business purposes, but protected from unauthorized alteration, deletion, or destruction and from environmental hazards.

An authentic record is one that is proven both to be what it purports to be and to have been created or sent by the person who purports to have created or sent it.

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

The trustworthiness of a record refers to its integrity, and to whether it is complete and unaltered.

A useable record is one which can be located, retrieved, presented, and interpreted, and which preserves the information content, context, and structure. It should be capable of subsequent presentation as directly connected to the business activity or transaction which produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

3.2.2. Records Maintenance and Use Requirements

Federal regulations require the following actions in this phase of the life cycle:

- Establish records systems for 'filing' or 'classifying' records and separating records from nonrecord and personal materials
- Specify official file locations and storage media for records of all types
- Provide reference services to facilitate access to records by authorized users
- Provide standards, guides, and instructions for easy reference to records
- Periodically review and audit recordkeeping systems and practices

See Procedures and Processes: 4.2.1. Filing Records in Recordkeeping Systems and Appendix D: Records Compliance Checklist and Instructions for detailed information on records maintenance, use, and auditing.

3.2.3. Categories of Bureau-wide Records Systems

In addition to records maintained on an individual's computer and a division's shared files, the Bureau maintains hundreds of shared Bureau-wide systems for the maintenance and retrieval of more substantive types of Bureau records that should be available to many or all employees. Information sharing is now a high priority for all Bureau employees, consistent with the top priority mission of averting terrorist attacks.

See Procedures and Processes: 2.2. Categories of Bureau-Wide Records Systems for a detailed list of Bureau-wide records systems and how to use them.

3.2.4. Retrieving Information from Bureau Records

3.2.4.1. Disseminating Records/Information outside the Bureau

Access to Bureau records is provided to the Congress, law enforcement entities, other Federal agencies, Federal courts, and the public in compliance with the following programs:

- Freedom of Information Act (FOIA) and Privacy Act (PA)
- National Name Check
- Mandatory Declassification Review
- Discovery

See Procedures and Processes: 4.2.3.1., for a detailed description of each of the items listed above for disseminating records/information outside the Bureau.

3.2.4.2. Storing and Retrieving FBI Records for Internal Use

Storing Records

FBI records are stored in field divisions, headquarters offices, and various other locations around the world. Most Headquarters closed-case files are stored at the Alexandria Records Center (ARC), which is managed by RMD's Records Storage and Maintenance Unit (RSMU). The Security Division is responsible for approving all storage locations. (See Open Storage Secure Area Checklist for a checklist of Secure Area Facility Requirements guidelines.)

FBI headquarters offices may send records to the ARC for storage if the records are not needed on a day-to-day basis in the originating office. Records that are used on a daily basis must remain in the office until they become less active. Additionally, administrative records that are covered by Classification 319 and are related only to individual unit activities (such as Time and Attendance records) may not be stored at the ARC. However, with the anticipated expanded storage capacity of the Central Records Complex (CRC), these records will be accepted for storage there.

Records with a classification higher than Secret or containing Sensitive Compartmented Information (SCI) may not be stored at the ARC.

Environmental Storage Policy

All records, whether paper, electronic, or digital, must be stored to meet environmental standards and preservation requirements.

Retrieving Records

Authorized Bureau employees may request files that are in storage. All requests for files, including personnel files, maintained by RMD at any location must be made through the File Automated Control System (FACS) in FBINET (FBI network). This ensures more effective and efficient control of the location and security of FBI Headquarters (FBIHQ) files. For detailed instructions on using the FACS system, select the link provided to the appendices to this manual. The individual to whom the file is charged out must be the requestor and user of the file, not a third party providing general records request assistance.

The individual to whom the file is charged out is responsible for the file until it is returned to RSMU. If the file is charged out to an individual and cannot be located, the individual's division director and the RMD Security Officer will be notified of the potential loss of FBI information. This could result in a security violation.

See Procedures and Processes: 2.3.2. Storing and Retrieving FBI Records for Internal Use for a detailed description of how to store records, including specific types of records, as well as the environmental requirements for records storage.

Returning Requested Files

All files must be returned to RSMU within 90 days of receipt unless the requestor requires additional time. To retain a file longer than 90 days, the requestor must recharge the file through FACS.

Files being returned to RSMU storage must be hand delivered to FBIHQ Room 1210 where information about them will be scanned into FACS to indicate their return. They will be sent back to the ARC by secured courier and returned to storage.

Restrictions on FBI Records

Bureau employees are required to respect all statutory, regulatory, and FBI policy requirements for the protection of sensitive and restricted information. Title 18 U.S.C. 798 provides fines and imprisonment for the unauthorized disclosure of national security classified information, and

Executive Order (EO) 12958 (and the Amendment to EO 12958) restricts access to such information. Only the originating agency may waive access restrictions and then only when essential for authorized and lawful Government purposes. Even in those instances, the agency must certify in writing that such access is consistent with national security. It also must ensure that the information is properly safeguarded and must limit access to documents essential to the historical research project or documents that the former Presidential appointee originated, reviewed, signed, or received while in office. Guidance on the application of national security classifications, caveats, and compartmented access requirements can be found on the Directorate of Intelligence and Security Division web sites.

In addition to specific security classifications, caveats and compartmented access restrictions, access to Bureau records, before the events of September 11, 2001, were also limited to those who had a need to know. The Director's mandate that FBI information must be shared more widely with law enforcement and intelligence partners across the world has led to a new Bureau-wide policy tilted toward information sharing. Only Assistant Directors can now approve the imposition of access restrictions in the Bureau's case management system (see EC Case ID #: 66F-HQ-A1307721 re: Restricting Cases In ACS).

Using Public Key Encryption (PKE) to control access to records

The FBI is implementing the use of smart cards that contain each FBINET user's digital identity and serve as the employee's building entry badge. The first FBINET application to use the digital identity technology is the Outlook e-mail application. On June 17, 2005, the Director signed the policy document providing guidelines for the use of digital identity tools (see EC Case ID #: 319-HQ-A1487698 re: Policy Development Working Files PKI - Digital Identity Guidelines).

Public Key Infrastructure (PKI) technologies, including digital signatures and message encryption, provide an additional level of protection from unauthorized access for certain types of FBI information. This policy defines those specific types of FBI documents that are appropriate for this additional level of protection. It is the responsibility of each FBI employee to identify those documents (in any electronic format, including e-mail) which should be encrypted, digitally signed, or both.

Generally use digital signature without encryption only when the substance of the communication is not sensitive, but the signature conveys an important authorization. Use both digital signature and message encryption when the substance of the document or communication is (1) sensitive and/or security classified and (2) refers to any of the following subject matter areas:

- Personal information regarding a personnel action (e.g., salary, medical condition/information, career board, merit promotion, selection system information, administrative inquiry, firing, security incident, managerial/performance deficiencies, Office of Professional Responsibilities (OPR) referrals or investigations)
- Sensitive cases, investigations, special projects/inquiries (i.e., Whistleblower cases, high level public official corruption cases, Office of the Inspector General investigations, security

incidents, shooting incidents, assets and informants, any sensitive internal investigations, or the 'sensitive stages' of any current investigation)

- Legal opinions
- Information requiring special handling (e.g., Special Access Program/Special Access Request, NOFORN, ORCON, sources & methods, Community of Interest)
- Fact sheets, talking points, question and answers, or briefing materials on issues that are sensitive or controversial, for which distribution should be limited to those with 'need to know' or for which timing of dissemination should be controlled and coordinated
- Specific information about the schedules and itineraries of the Director and other senior FBI officials
- System security testing results (i.e., certification test reports and penetration test reports which identify security issues that pose a risk to identified systems) or assessment results (i.e., vulnerability assessments and risk assessments which identify the system, and the CJIS Computer Security Incident Response Capability (CSIRC) information)
- Contracts (e.g., statements of work, sole source justifications, independent government cost estimates, solicitations)

3.2.5. Auditing Records Compliance

3.2.5.1. Records Self-Audit

To ensure that Bureau files are managed effectively, each division and office is encouraged to conduct a Records Audit on an annual or biannual basis. Records Audits assist the division by identifying problems early so that they do not become significant deficiencies identified in Inspections or other Records Management Division evaluations. The Records Audit is similar in many ways to the standard File Reviews conducted by Supervisory Special Agents in that the Records Audit reviews the accuracy and completeness of the records uploaded and indexed in the Automated Case Support System. However, while the primary purpose of a File Review is to assess the management of a case by the case Agent, the primary purpose of a Records Audit is to assess the arrangement, description, completeness, and disposition of the files themselves. A Records Audit includes records in all formats (paper, electronic, audiovisual, other), administrative as well as investigative and intelligence records, and current as well as closed case files. In most cases, Records Audits are conducted by the division's Records Management Liaison, under the supervision of the Administrative Officer. The checklists used for Records Audits are also provided to the Inspection Division for their use as part of Program Reviews. See Appendix D: Records Compliance Checklist and Instructions.

3.2.5.2. Records Control/Inventory

In addition to the periodic Records Audits conducted by each division or office and the records reviews conducted within the scope of a periodic Inspection Division (INSD) inspection, the Records Compliance Unit is developing a new program to conduct evaluations of records management practices throughout FBIHQ and field division offices.

Within the decade, RMD will have a new state-of-the-art Central Records Complex (CRC) that will provide sufficient storage space to contain all closed case files from all divisions throughout the Bureau. In the interim, the Records Compliance Unit may take custody of pre-1991 closed case files from all divisions through the Records Control Project upon formal request by electronic communication (EC), from the SAC or Division Assistant Director to the Chief, Records Policy and Administration Section, RMD. The divisions moving to new headquarters receive priority consideration.

3.3. Records Disposition

Disposition is the third and final stage in the life cycle of records. The term 'disposition' refers not only to the destruction of records, but also to other actions that occur to records at the end of their life cycle. Records that have been determined to be historically valuable are transferred to NARA at the end of their life cycle. Records that do not have the same historical significance are destroyed or disposed of after a prescribed number of years.

3.3.1. Records Disposition Program

The Bureau's records disposition program manages records during the final stage of their life cycle. Elements of a records disposition program include the following:

- Development of retention schedules for all records
- Supervision of the storage of inactive records
- Management of the disposal of temporary records
- Transfer of permanent records to NARA

Most records cannot and should not be kept forever or even for long periods of time. All records, regardless of their format (paper, electronic, CD-ROM, diskette, etc.), fall into one of two categories for disposition purposes: temporary or permanent.

3.3.1.1. Temporary Records

Temporary records are records that are deemed by the National Archives and Records Administration to have no continuing value after their usefulness to the agency has ceased. These records are not transferred to NARA for preservation but rather are destroyed either after a fixed period of time or after a specific event has occurred. Their retention period may range from a few months to many years. Many of the Bureau's administrative and some mission-related records are temporary. Most of the records filed in Classifications 319 and 67Q are temporary records.

Disposition instructions for Classification 319 and 67Q records can be found at [redacted] b7E

3.3.1.2. Permanent Records

Permanent records have been determined to be sufficiently valuable for historical or other purposes; therefore, they warrant continued preservation by the Federal government after their usefulness to the Bureau has expired. Nearly every investigative and intelligence file classification contains some permanent records.

Example: Many bank robbery investigations filed in Classification 91 are permanent and will eventually be transferred to NARA.

3.3.1.3. Unscheduled Records

Records that have not been determined to be either permanent or temporary are called unscheduled records. These records have no authorized retention, destruction, or transfer instructions. Therefore, unscheduled records must not be destroyed. They must be kept until a retention schedule is approved for them, authorizing destruction or transfer to NARA. Unscheduled records should be reported to the Records Disposition Unit (RDU).

3.3.2. Records Scheduling

Federal records may not be destroyed or removed from the FBI without the approval of the Archivist of the United States, who oversees NARA. The Director and other high level Bureau officials do not have the authority to determine when records can be destroyed. The Archivist is the only individual in the Federal government with the authority to approve the destruction or deletion of records.

Disposition authorities represent a legal agreement between the Bureau and NARA that provides guidance for disposing of records that have met their retention requirements as well as instructions for identifying and transferring historically significant records to the National Archives. In addition to the disposition authorities for each file classification, disposition authorities are being developed for the Bureau's electronic information systems and other records that fall outside the file classification system. For example, a disposition authority has been approved for the National Crime Information Center (NCIC) electronic information system. RMD's RDU is responsible for developing records disposition authorities for the FBI's records. (See Procedures and Processes: Section 3.3. Applying the FBI's Disposition Authorities.)

4. Procedures and Processes

Procedures and processes describe the specific actions to be taken to accomplish the records life cycle policies outlined in the previous section. This section contains links to a variety of tools that provide more in-depth guidance on subjects covered.

4.1. Records Creation and Receipt

4.1.1. Definition of a Record

Records in the Federal government are defined in statute and regulation (see 44 USC § 3301) to include all documentary material, regardless of physical form or characteristics, made or received by a Federal agency or its contractors, in connection with the transaction of that agency's official business, that is either preserved or appropriate for preservation because of its administrative, legal, fiscal, or informational value. See the following records terminology definitions.

Documentary materials: A collective term for media containing recorded information that can be records, non-record materials, or personal papers, regardless of the media used to store them or the methods or circumstances of recording

Regardless of physical form or characteristics: The physical storage medium may be paper, CD, videotape, or other recordable media. The method of recording the information may be manual, photographic, electronic, or other recordable technologies

Made: The act of having created or recorded information in the course of official business

Received: The acceptance or collection of documentary materials in the course of official business, regardless of their origin (for example, other FBI offices, other Federal agencies, private citizens)

Preserved: The filing, storing, or otherwise systematically maintaining documentary materials in the course of official business

Appropriate for preservation: Documentary materials made or received by an agency in the course of official business that should be filed, stored, or otherwise systematically maintained because of the evidence of agency activities or information they contain, but that may not be covered by current filing or records maintenance procedures

Questions to ask in determining record status:

- Was the creator or recipient acting in an official capacity? Was the document (paper, electronic, or other media) created or received by a Bureau employee on Bureau time using Bureau equipment and materials?
- Does the document contain substantive information about Bureau business?
- Was the document created to conduct Bureau business and circulated or communicated to others?

- Was the document used to conduct Bureau business or was it retained only for reference purposes? Is it a convenience copy or the original document?
- If the document was retained as a reference or convenience copy have any notations containing substantive information subsequently been added?
- Was the document placed or uploaded into Bureau files or was it kept in an individual employee's possession? (For instance, rough notes or reference materials are not normally a part of the file.)
- Was the document serialized and uploaded into ACS as part of a case file? (Documents do not have to be serialized or part of a classification in order to be a record).
- Does the document subject matter fall under a Bureau classification number? (For example, is it related to a bank robbery investigation under classification 91?)
- Why was the document created in the first place? Does the Bureau have recordkeeping requirements directing its creation?

The considerations that identify the circumstances of a document's creation, maintenance, and use help to determine the record status of a document.

Additional resources to help determine record status:

See Managing the Records of FBI Executives for guidance and information on managing records and personal files of high-level officials

See PowerPoint presentation, 'What's a Record?'

Contact RMD with any suggestions, comments, or questions through RMD's feedback form

4.1.2. Definition of a Non-Record

Non-record Materials are documentary materials that are owned by the U.S. government but are excluded from or do not meet the legal definition of Federal records. According to 44 USC 3301, non-record materials include:

- Library and museum materials made or acquired and preserved solely for reference or exhibition purposes.
- Extra copies of documents preserved only for convenience of reference.
- Stocks of publications and processed documents (i.e., forms). Note: this does not refer to the record set of publications or forms.

Not all copies of records are non-record material. Copies of documents that meet the definition of a record are used for different purposes within the Bureau. For example, a copy of a Division's budget report may be maintained in the Division's files as part of its administrative records. It may also be a record in the Finance Division as a feeder report for a Bureau-wide budget report. A non-record copy may also become a record if substantive notes or comments are added to the document.

Non-record material does not need to have an authorized disposition. However, it should be filed separately from records and purged periodically. Examples of non-record materials include technical publications, supplies of frequently used forms, etc.

Personal Files are documentary materials belonging to an individual that are not used to conduct agency business. Characteristics of these types of files include the following:

- Related solely to an individual's own affairs or used exclusively for that individual's convenience
- May be in any format or on any media (e.g., e-mail)
- Also called personal papers or personal records
- Should be maintained separately from office records

Personal files may be disposed at the discretion of the owner. For example: an individual employee's copy of his or her SF 50; an e-mail inviting co-workers to an anniversary celebration.

4.1.3. Office Responsibility for Recordkeeping

To determine which recordkeeping requirements are the responsibility of an office, address the following questions:

- What programs is the office responsible for managing?

  In many cases, program responsibilities and the records resulting from them are clearly delineated. However, in carrying out the Bureau's business, offices often have similar and even overlapping responsibilities. This may result in duplicate recordkeeping systems if staff are unsure which office is the official record keeper.

- Does the office have a Bureau-wide responsibility for a particular administrative function?

  For example, the Finance Division has the overall responsibility for the annual budget and appropriations reports, and is responsible for maintaining these records.

It is much easier to determine responsibility for managing the records of a particular investigative case when the Office of Origin (OO) has overall responsibility for cases opened in its jurisdictions.

4.2. Records Maintenance and Use

4.2.1. Filing Records in Recordkeeping Systems

Records management policy and practice assigns individual record items to groups. After a document has been created or received, and has been identified as an FBI record, the original (or 'record copy') must be grouped (or 'filed') with similar records for efficient management, retrieval, and disposition. Filing can be associated with paper files or refer to a 'drag-and-drop' process to move an electronic file from one computer folder to another. Once assigned to a group (or 'record system'), records are indexed, identified as either active or inactive, moved to offsite storage, then destroyed, deleted or transferred in accordance with the legal authorities associated with their record system or group. The filing of individual record items in records systems

continues to be a fundamental requirement of the management of all types of FBI records, including paper, electronic, audiovisual, etc.

4.2.1.1. Definition of a Record Copy

When there are multiple copies of a record available, the official document (or 'record' copy) must be identified, protected from change or loss, and maintained in the appropriate filing location. In the paper records environment, it is usually possible to identify the 'original' record (usually the paper with original signatures) and file it in the appropriate records location. In the electronic world, any authentic and reliable copy from a trustworthy information system could be treated as the record copy.

For investigative and intelligence records, the case file of the Office of Origin (OO) is the appropriate filing location for documents related to that case, regardless of which division or office creates the document. For administrative records, the filing location for the record copy depends on which division/office has Bureau-wide responsibility for the function represented. For example, inasmuch as the Finance Division (FD) has overall responsibility for annual budget and appropriations reports, FD would maintain the record copies of budget documents (Filing Classification # 319D3). The copies of budget documents in other divisions/offices are convenience copies only.

4.2.1.2. Record Groups and their Filing Locations

Records are filed according to their content and use. There are two general types of content: administrative and program. Administrative records facilitate routine organizational and housekeeping activities and are created by all units within the FBI. Examples of administrative records are time and attendance registers, travel vouchers, purchase orders, and budget preparation documents. Most administrative records are covered by Classification 319.

Program records are mission-related documents that are created as a result of the FBI's unique investigative and intelligence functions. Examples of program records include investigative or intelligence documents relating to terrorism, white collar crimes, violent crimes, or other actual or potential violations of law, and include most of the Bureau's more than 300 separate filing classifications as listed in the FBI Investigative Classifications.

Both administrative and program records fall into three categories:

- Transitory, non-substantive records that are for short-term use only may be maintained on an individual's office computer or in local paper files. These files may be purged in accordance with routine e-mail or e-files purge schedules, when no longer needed by the individual.
- Transitory, non-substantive records that are available to other people within the same squad/office/division should be filed in a shared drive or that office's shared paper files. Mostly administrative in nature, these files should be retained as long as required by the administrative file retentions defined in the 319 classification guide.
- Records with substantive information relating to a case or to Bureau policies, procedures, and activities, and records that would be of interest to other offices or divisions must be serialized

and uploaded into the Bureau's general case management system. These records are retained in accordance with specific time schedules established for each classification by NARA.

In general, most administrative records fall into the first and second categories above. Most investigative records fall into the third category. Most intelligence records are filed in either the general case management system or specific Bureau-wide systems for the preparation and dissemination of intelligence reports (such as the FBI Intelligence Information Report Dissemination System [FIDS]).

4.2.1.3. Definition of a Case File

The majority of the FBI's mission-related, or program, records are arranged in case files related to a specific investigation or intelligence matter. The FBI filing classification numbers relate to particular areas of investigation, law enforcement, intelligence gathering, or other responsibilities of the Bureau. Often, a classification number is tied to the legislation that enacts a particular type of investigation or other Bureau activity. Case files that are related to a filing classification are assigned unique numbers consisting of the classification number, the OO designator, and a chronologically assigned number. See the FBI Investigative Classifications – FY 2007 for a complete list of Bureau Classifications.

The individual documents that are included in each case file are referred to as serials. Documents are assigned chronological numbers as they are added to the file. Once a document is serialized into a file, it is considered part of the case file. Documents kept in paper based recordkeeping systems are serialized by handwritten notation as the documents are added to the case file.

Documents that are appropriate to serialize as part of a case file meet the following criteria:

- They meet the definition of a Federal record
- They contain information pertaining to that specific case file
- They are unique; in other words, they are not a duplicate of records already serialized in the case file

4.2.1.4. Working Files

Working files are the files that Bureau employees create as they generate a report, publication, or other record. These files are generally not considered records because they consist primarily of drafts of reports, studies, policies, discussions, and other materials that are not significant or unique enough to be included in a case file. In most instances, these materials can and should be discarded when the case is closed or the report is finished. However, the most recent draft of a report or other document must be retained until the final is completed. In some circumstances, drafts of high-level policies, decisions or directives may be retained, at the discretion of the originating office, in order to document the process by which the document was formulated.

All Bureau employees creating working files are responsible for their identification as such and separate maintenance from case files or other official file records. Working files that do not meet the criteria for records should be maintained separately as non-record materials and periodically purged when no longer needed.

4.2.1.5. Transitory and Tickler Files

Many copies of records and non-records are kept for short periods of time until a specific action has occurred, after which the file or document no longer has value. For example, you might keep an extra copy of outstanding leads assigned to your office or squad to serve as a tickler file—a file that reminds you of actions required and provides a copy for quick reference purposes only. Many e-mail messages can be characterized as transitory correspondence, which should be routinely purged once its usefulness has ended. Consult the guide When Are E-Mails Records? for more information on determining whether an e-mail is a record.

4.2.1.6. File Plan

For records maintained in division paper files or a shared electronic directory within an office/division/squad, it is very important to arrange the folders in an organizational schema, termed a 'file plan.' A file plan is a road map or table of contents of an office's records. The plan shows every classification number or file series maintained by the office, regardless of the record's location. The plan should identify records in all media, including paper, electronic, and audiovisual, that are physically stored in the office: electronic records, whether on a local or remote server or on removable media such as CDs; records on other non-paper media such as DVDs, audiotapes, or film; and records stored in other office file storage areas. Only records should be identified on the file plan, not non-record materials such as reference files. Records described on the plan should include not only those originated in the office, but also any others that are received or otherwise acquired and used in the course of business.

The file plan lists the 'folders' in the paper files or the electronic shared drive, with the calendar or fiscal year associated with the creation of each one. Whenever possible, the folder names should be drawn from the Bureau's file classification system. Each year, the previous year's folder should be closed and moved to an offline or offsite location. If the subject matter continues to be needed in the filing system, a new folder should be opened for the current year. This periodic 'cutoff' process may be established at other than annual intervals (e.g., biannually) as long as it is an established chronological period and completed regularly. See Procedures and Processes: 2.1.7. What Is a File Cutoff?

When a division's paper files or shared drives are organized in accordance with the file plan guidelines listed above, it is easy to periodically move inactive and non-current files out of an office area to storage locations, freeing up needed office space. It is also easy to conduct 'E-Files Clean-Up' Days to eliminate the obsolete and redundant electronic files that make litigation response and the electronic discovery process difficult and expensive.

The file plan for each shared directory or records storage location should be posted at the beginning of the shared drive or paper files, and must be available for inspection for records audit purposes. File plans should be updated as needed, and offices are required to provide RMD a copy of their current file plan each year at the time of the files clean-out day.

Below is an example of a File Plan form. For a sample detailed file plan, see Appendix F: Detailed Sample File Plan.

FILE PLAN			
1. Office:	2. Phone:	3. Rm. No.:	4. For FY:
5. Prepared by:	6. Approved by:		7. Date:

Classification or File Series Number (including Alpha and Item #	Classification or File Series		Location	Disposition Instructions	Vital Record
	Title	Description			Yes / No

Figure 1. Sample File Plan

4.2.1.7. File Cutoff

The point when files change from active to closed, or inactive, is referred to as a file cutoff. The purpose of file cutoffs is to identify and control records in manageable blocks, usually either by fiscal or calendar year.

The purpose, use, and arrangement of the records determine the file cutoff procedures. Most file cutoffs are determined either by date or by occurrence of an action or event. For some files, an event, such as completion of a project or discontinuation of an investigation, causes the file to be closed. Other files are accumulated based on an ongoing activity, such as office budget, time and attendance, or procurement files.

For most case files, an action or event causes files to be closed. This can occur at any time during a particular year. It is then necessary, on a yearly basis, to weed out those files that have closed during the year and physically transfer them to an inactive storage area. In this way, all cases closed at any time during the year are cut off at the same time and identified as part of the block of files belonging to that year.

Some files do not have event-driven cutoffs; that is, there is no specific action or event that must occur in order for the files to be closed. These files must be identified and cut off based on their age. Many administrative files are not managed as case files and are not cut off based on an event or action. These files are usually only needed in the office for business purposes for a year or two. They may then be physically removed to closed or inactive file storage for the remainder of their retention period. However, they often accumulate in offices as ongoing files dating back many years, since no cutoffs are ever applied. For records such as these, that are maintained continuously, a cutoff must be imposed, usually on a calendar year basis. Soon after the end of each calendar year, file managers will be notified of a 'file clean-out day' on which all inactive records will be removed from the files and new files will be set up for the coming calendar year. In this way, just as in case file management, the records can be identified and managed in chronological blocks.

Block Closed Records

Perhaps the most crucial function of file cutoffs is to provide a starting point from which the records retention period can begin. All Federal records must have disposition authority from NARA. In simple terms, this means that all Bureau records will be retained for a period of time, then either destroyed or transferred to NARA for permanent storage. The length of time that the records must be kept before either transferring or destroying them begins at the point of the file cutoff. For example, time and attendance records have a retention period of six years. Following the cutoff procedures of removing each year's accumulation of files to inactive storage will make it easier to determine when a block of records is six years old and may be destroyed. If, however, files are left to build up year after year, finding those that are eligible for destruction each year will be much more difficult. Similarly, if case files that are closed during a particular year are systematically removed and kept together by year, it will be much easier to identify them when the time comes either to destroy or transfer them to NARA.

Implementing a File Cutoff

Ongoing Files (non event-driven)

- When setting up files, determine the retention period for the records series. In other words, when are these records eligible for destruction? One year? 18 months? Three years? The 319 Guide identifies the retention period for most administrative records.
- Write on the outside of the file jacket or folder the Classification number; alpha, and item number (if applicable); title as it appears in the Classification Guide; and the calendar year.
- File all appropriate material in that file until the last document on December, 31 20xx. Note: if a volume/section becomes too bulky before the end of the calendar year, begin a new volume/section identified with the same information, and mark it volume/section 2.
- On January 1 of the following year, start a new volume for that file, and under the file number write the new calendar year. All new documents are placed in this volume (or volume 2,3, etc. if needed) for the remainder of the year.
- Close out the previous year's volume and remove it from the files. Closed volumes may still be needed close at hand. Based on office needs, closed files may be stored in a closed files storage area, or elsewhere in the office, as long as they are properly identified.
- On the closed file front or folder, you may use the closed date to calculate the time remaining before the records are eligible for destruction. For example, if the retention period is 'Destroy when one year old,' you can determine that the records can be destroyed at the beginning of the next calendar year. In this case, write "ELIGIBLE FOR DESTRUCTION 1/1/20xx" on all closed volumes. This date is one year after the last document in that volume.
- Continue this cutoff cycle every January, starting a new section and closing the previous year's cycle.
- Each year, RMD will send a notification of administrative records that are eligible for destruction. After receiving the RMD notification, consult your closed files to determine if any are eligible for destruction (as marked when closed). Segregate eligible files and destroy in accordance with RMD instructions. Note: RMD will coordinate the destruction of electronic copies in ACS.

Event-driven or Contingent Cutoffs

Records that are closed after a certain event or action are handled somewhat differently than those that are ongoing and have cutoffs imposed. For example, the disposition instructions for 319B20, Contract Appeals, are 'destroy one year after final action on decision.' This may occur any time during the calendar year. Some cases in a file may remain open for years; others may be resolved and closed quickly. For these records do the following:

- Identify folders as above
- During the year, as a case is closed, mark 'closed' on the folder or file front

- At the end of the year, remove all cases closed during that year. Maintain all closed cases from that calendar year together
- Determine the records' eligibility for destruction. Calculate this based on the date of the last day of the calendar year, not the day the case file was closed. Mark "ELIGIBLE FOR DESTRUCTION 1/1/20xx" on all closed volumes

Unscheduled Administrative Files

Some administrative records do not have authorized retention periods. (See example in Classification 319 Guide at 319J-12, Occupational Safety and Health Matters.) For these records, establish yearly cutoffs but do not write an 'Eligible for Destruction' statement on the files.

By following these steps, you effectively group documents within a file by their destruction time period, and you can easily identify and retrieve those documents eligible for destruction.

Managing Cutoffs in Electronic Information Systems

File cutoffs are also executed in electronic information systems, depending on the structure and purpose of the system. Some data files, like paper files, are needed for current business for only a year or two, and then become inactive. These data files can be moved to inactive storage, offline, or nearline for the remainder of their retention period.

Sometimes, the information system includes a history file to which inactive records are moved. Other data files contain records that are needed on an ongoing basis, so that many years of accumulated data may be considered still active.

As with case files, most of the records in Bureau information systems have event-driven cutoffs. For example, records may be destroyed after the case is closed or the subject is apprehended.

When establishing cutoff periods for electronic information systems, it is important to plan for the implementation of cutoffs for the life of the system.

See Appendix E: File Cutoff Examples.

4.2.2. Categories of Bureau-Wide Records Systems

4.2.2.1. Central Case Management System

The FBI uses a central records system for maintaining its substantive investigative, intelligence, personnel, applicant, administrative, and general files. This system consists of one numerical sequence of subject matter files (termed 'classifications'), an alphabetical index to the Universal Index files (termed the 'UNI'), and a supporting system Investigative Case Management (ICM) to facilitate processing and accountability of all important mail and other types of documents placed in files. Investigative and intelligence documents relating to specific cases, as well as significant administrative documents appropriate for distribution outside divisions, are entered as serials into Bureau-wide case files, printed out for placement in the paper case files, and uploaded electronically into a data file available to authorized users. Working papers and drafts relating to subjects covered in the case files, as well as less important administrative records, are maintained within divisions, units, squads, and other subordinate groups in local filing locations.

The 300+ classifications used by the FBI in its basic filing classification system pertain primarily to Federal violations over which the FBI has investigative jurisdiction. However, included in the classifications are intelligence gathering, personnel, applicant, and administrative matters to facilitate the retrieval of significant documents.

Each case opened under a particular filing classification is primarily 'owned' by one field or headquarters division—this owner is the Office of Origin (OO) for that case. All of the actions reported on that case are serialized and uploaded into the one OO number for that case, even if other divisions/offices are creating and serializing the documents.

A typical case file number consists of a three-digit classification number, a one- or two-digit alpha designation for subdivisions under that subject, a two-letter designation for the OO, and then a case number assigned sequentially by the system. (Example: 91A-BA-124576).

Control Files are opened for the purpose of administering specific phases of an investigative matter or program. Control Files are not created for every classification. These files are designated with the letter 'C' before the case number. (Example: 29B-NF-C4456).

Miscellaneous documents that do not rise to the level of opening a case are filed as Zero (0) files. Zero files are opened for every investigative or intelligence classification. (Example: 315-0)

Each document within a case is assigned a consecutive number (serialized) at the time the document is indexed into the system. Whenever possible, the text of the document should also be 'uploaded' into the system so that all of the information in the document can be made available to all authorized users.

- Documents such as ECs should not be uploaded until all those listed on the approval lines have initialed the document or otherwise provided their concurrence. Increasingly, documents are being circulated by e-mail for concurrence rather than disseminated in a single paper copy for initials by all. When this is the case, the copies of the e-mail concurrences should be printed out and filed in the paper case file, attached to the document approved. It is not necessary to upload the text of these concurrences.
- Attributes of the document must not be changed during the uploading process because changing the attributes makes the electronic document different from the actual paper copy.
- Working or reference copies of the document should not be made until all signatures or concurrences have been obtained, the document has been uploaded, and the serial number has been placed on the document.

The Information Technology Operations Division (ITOD) creates a monthly report indicating the percentage of documents serialized in ACS with and without text. This report can be found on the ITOD website.

ITOD has created a web-based application (WACS) to simplify and facilitate the uploading of documents into ACS. WACS provides a point and click method of uploading documents and eliminates the previous manual step, which required that documents be converted to ASCII prior to uploading.

The major components of ACS are as follows: the ICM, the Electronic Case File (ECF), and the Universal Index (UNI).

4.2.2.1.1. Investigative Case Management (ICM)

ICM provides a single source for opening, maintaining, and closing cases; creating initial serial and subject indices for a new case; setting and tracking leads to any FBI location; setting ticker reminders; facilitating file reviews; and maintaining case reference information.

4.2.2.1.2. Electronic Case File (ECF)

ECF serves as the central electronic repository for the FBI's official investigative textual documents. ECF provides the capability of uploading word processing documents to the mainframe where they are filed and serialized, parsing uploaded documents for structured document fields and lead information, searching documents by both structured (i.e., formatted fields such as From/To) and unstructured (i.e., full text) means, and downloading documents in their original word processing format. ECF also handles the serialization of non-textual records.

4.2.2.1.3. Universal Indices (UNI)

UNI provides on-line support for indexing and searching investigative, intelligence, and administrative case files' subjects and references using a single centralized database environment. In the first serial in a case, the case agent or analyst circles terms that represent the subjects of the case, and underlines terms that represent others who are merely references in the case. The records specialist uses these notations to establish the index records in UNI.

4.2.2.1.4. Universal Case File Number (UCFN)

The case number used for the Bureau's central case management system is a universal number, assigned sequentially by the computer program. In April 1991, the FBI converted to a system whereby only one file number was used for each investigative case, and the number was owned by the office primarily responsible for the case (OO). It is Bureau policy to maintain only one record copy of each document serialized in ACS, with pointers or cross references as necessary. Unfortunately, many offices have duplicated records already existing in ACS by uploading their convenience copies into other case files. This unnecessary duplication has made it more difficult for the Bureau to comply with document requests resulting from public access statutes or litigation, and has resulted in overloads to both our electronic storage systems and the associated paper case files. Therefore, offices are advised to file only one record copy of each document in the appropriate case.

Prior to April 1991, each office (OO or Lead Office) involved with an investigation or intelligence matter opened a separate investigative file on the subject and maintained the file within the office. For major cases, this resulted in over 56 different file numbers for the same subjects and a large amount of unnecessary duplication.

4.2.2.1.5. Documenting Leads

One of the important facilities provided by the Bureau's central case management system is the ability for one office to assign follow-up tasks to other divisions/offices in investigative, intelligence, or administrative matters. A lead is currently set using the macros provided by

Electronic Communications. Leads may be automatically set through parsing of the lead section from an EC, manually set by an employee typing the lead information required into the correct fields, or set from another document. When covering leads that require action, the tasked office may not simply indicate 'read and clear' on the lead. A lead with a tasking requires the action to be performed and a response to be prepared. The response can be documented by entering the action that was taken in the Lead Disposition field, or a response document may be prepared to indicate the action taken. When covering a lead by preparing a response document, offices are required to enter the file number and serial of the response communication in the covered lead section of the original request in the case management system.

4.2.2.1.6. Preparing an Electronic Communication (EC)

When preparing ECs, the title of the EC must match the title of the case file number being used. To determine the title, access ICM and type the file number you wish to use on your EC. Take note of the title and use it on the EC. When preparing an EC using a Classification 319 or 67Q case file number, use the title given in the 319 Guide or 67Q Guide.

The Synopsis field should be no more than two lines. When the Synopsis field is automatically parsed to ACS, there is only enough room for approximately two lines of text from the EC.

When preparing response ECs, the writer must include the originator's file number and serial in the reference field. In addition, the originator's file number must also be placed in the Case ID field of the EC.

If copies of the EC are necessary, they should not be made until after the EC has been approved and uploaded, and the serial number has been written on the original signed document.

4.2.2.2. Intelligence Reports Records Systems

An Intelligence Information Report (IIR) is a raw intelligence report in the form of an electronic organizational message transmitted through the FBI's secure messaging system. It is a specially formatted message that provides the means for appropriate dissemination of unevaluated intelligence within the U.S. intelligence and Federal law enforcement communities. For instructions on the format and process for preparing, submitting and disseminating IIRs, consult the FBI Intelligence Information Report Handbook.

The FBI has a mandate from Congress, the President, the Attorney General, and the Director of Central Intelligence (DCI) to produce intelligence in support of its own investigative mission, national intelligence priorities, and the needs of other intelligence consumers. The FBI serves a considerable customer base, ranging from its own investigators and executives to other U.S. government departments, state, local and tribal law enforcement, as well as the general public. The IIR is the vehicle through which raw intelligence is shared within the FBI and the intelligence and law enforcement communities.

4.2.2.3. ELSUR Records System (ERS)

Electronic Surveillance (ELSUR) Records is the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other

device. The FBI's ELSUR Program consists of the following four components directed by various HQ divisions:

- Legal matters pertaining to criminal investigations are the responsibility of the Office of the General Counsel, Investigative Law Unit. Legal matters pertaining to noncriminal investigations are the responsibility of the Office of the General Counsel, National Security Law Unit
- Technical matters are the responsibility of the Laboratory Division
- Operational matters pertaining to criminal investigations are the responsibility of the Criminal Investigative Division. Operational matters pertaining to noncriminal investigations are the responsibility of the Counterintelligence Division
- Oversight of recordkeeping matters pertaining to Title III ELSUR usage in criminal investigations are managed by RMD's ELSUR Operations Unit

ERS is an alphanumeric and numeric index containing the names of individuals and entities who have been the targets of electronic surveillance coverage sought, conducted, or administered by the FBI pursuant to a court order, consensual monitoring, or other authority. The system identifies (1) those who have been a party to a communication or present in a locale monitored/recorded electronically allowing such surveillance; (2) those who own, lease, license, hold a possessory interest in, or commonly use the property or location subjected to such electronic surveillance; and (3) those involved in the administration of the electronic surveillance. For example, the judge issuing or denying an order for an electronic surveillance application, the prosecuting attorney, and the official who authorized the initial filing of the application would be identified

ERS is comprised of four types of records:

- Principal records identify, by true name or best known name, all persons, entities, and facilities that have been the targets of electronic surveillance coverage sought, conducted, or administered by the FBI according to a court order. These records include, but are not limited to, persons, entities, and facilities named in an application filed in support of an affidavit seeking a court order to conduct or administer an electronic surveillance. Principal records may also include descriptive data associated with the name appearing on the record.
- Proprietary Interest records identify entities and/or individuals who own, lease, license, hold a possessory interest in, or commonly use the property or location subjected to an electronic surveillance. Proprietary Interest records may also identify individuals involved in the administration of the electronic surveillance—for example, the judge issuing or denying an order for an electronic surveillance application, the prosecuting attorney, and the official who authorized the filing of the application. Proprietary Interest records may also include descriptive data associated with the name appearing on the record.
- Intercept records identify, by true name or best known name, individuals who have been reasonably identified by a first name or initial and a last name as being a party to a communication monitored/recorded electronically pursuant to an electronic surveillance.

Intercept records also identify entities that have been a party to a communication or present at a local monitored/recorded electronically pursuant to an electronic surveillance. Intercept records may include descriptive data associated with the name appearing on the record.

- Reference records identify, by partial name such as a first name only, last name only, code name, or alias, those individuals who have been a party to a communication or present in a locale monitored/recorded electronically pursuant to an electronic surveillance, and may include descriptive data associated with the individual. If the individual is later identified by a more complete name, e.g., through further monitoring or normal investigate procedures, the reference record is modified to reflect the more complete name and converted to an Intercept record.

  See the frequently asked questions relating to the administration of both Title III and FISA ELSUR programs at [redacted] b7E

4.2.2.4. Personnel Records Systems

Superseded by Policy Notice #0165N, titled "Personnel Records," dated 02/11/2009.

Effective Date: 02/11/2009

4.2.2.5. Top Secret/Sensitive Compartmented Information (TS/SCI))

Receipt: Immediately upon receiving TS/SCI documents/materials, take them directly to the Security Officer for control.

Control: Use form FD-501 (manual and automated) for the receipt of TS/SCI material that will stay within the receiving office. Use form FD-502 (manual and automated) for the dissemination of TS/SCI material that will leave the receiving office and be transported to another location.

Dissemination: TS/SCI must be transported by an approved courier. Acquire courier letters from the Security Division.

Records Creation: TS/SCI documents destined for FBI files must be serialized with attributes only. The text of TS/SCI documents is prohibited from being uploaded into ACS. For instructions on serializing TS/SCI documents into ACS, see How Do I Upload a Document into the Automated Case Support System?.

Storage: TS/SCI must be stored in an approved Sensitive Compartmented Information Facility (SCIF). Security Division approves SCIFs for storage of TS/SCI material. G material must be maintained separately from other SCI material. G material may be filed in a folder behind the other SCI material; it cannot be intermingled in the same folder as other SCI.

Maintenance/Disposition: TS/SCI records material must follow the same disposition guidelines as other FBI record material.

4.2.2.6. Executive Correspondence

Correspondence to the FBI from Congressional, Department of Justice, White House, and other executive sources is received, disseminated for response, and reviewed by RMD's Executive Secretariat (ExecSec). Executive correspondence received from external sources as well as

memoranda, correspondence, letters, and other documents received by, signed by, and reviewed by the Director are maintained in an electronic recordkeeping system (Records Management Application or RMA) managed by ExecSec. Paper copies are maintained for a short period of time for convenience only.

Congressionals include correspondence written to the FBI in general or to any FBI employee or the Department of Justice (DOJ) by members of Congress and/or their staffs. Executive level correspondence includes correspondence written to or signed by the Director, the Assistant Attorney General of the Office of Legislative Affairs, the Associate Attorney General, the Deputy Attorney General, or the Attorney General, Department of Justice. While senior level managers prepare correspondence for the Director's signature, the record copy of all executive level correspondence is maintained in the RMA.

In addition to the copies maintained in the RMA, copies of responses to Congressional correspondence are maintained in the following file locations in the Bureau's case management system: [redacted] b7E

To assist senior management officials in managing their correspondence and their office files, RMD (RPAS) has published a guide entitled Managing the Records of FBI Executives. This guide provides basic information to distinguish Federal records from other documentary materials, including personal (or private) files.

4.2.2.7. Forms

RMD's Forms Desk manages the FBI forms program by ensuring that all Department of Justice (DOJ) and other government standards and guidelines are followed in the design and use of FBI-use-only forms. The DOJ policy for design of forms is contained in the DOJ Graphic Standards Manual. The FBI also follows additional government guidelines which have been issued by the Joint Committee on Printing (JCP) Government Printing and Binding Regulations, the Office of Management and Budget (concerning public-use forms), the Federal Register, and the Paper Reduction Act of 1995.

RMD's goal is to provide all users with electronic versions of forms. With the help of ITOD, a software design package has been selected to allow information to be gathered and displayed in dynamic forms (e-Forms) to provide users with the options to electronically fill out, save, and route forms online. Users are provided a central location where they can search an index for Bureau approved forms by title or by number.

4.2.2.8. Electronic Records

The data processing industry uses the term 'electronic record' to refer just to a particular set of fielded data. However, Federal records management laws and regulations define electronic records as all records created or maintained in electronic storage media in the course of official business that document significant policies or transactions of the government and are retained as evidence of transactions or for the value of the informational content. Electronic records may include information and data sets in all media, including databases, electronic mail, word processing, spreadsheets, CDs, DVDs, audiotape, HTML-web site records, voicemail, etc. There is no electronic medium that is exempt from the requirements of the Federal Records Act,

including all of the requirements listed in this manual relating to the creation, maintenance, and preservation of records. As with paper records, however, electronic records of other organizations or individuals that are seized for investigative or intelligence purposes may be treated as evidentiary property, not as records, and returned at the completion of the related case or closure of the investigative or intelligence matter.

4.2.2.8.1. Electronic Records Requirements

Migration

There is no permanent electronic medium. All electronic records will eventually become obsolete and inaccessible and must be migrated to a new storage media, database, processing software, etc. Because the migration schedules for all electronic media must be managed and accessible for software and storage media updates, electronic records (CDs, DVDs, floppies, audio tapes, etc.) should never be intermingled with paper files. Electronic records may be stored in climate-controlled office environments if segregated from paper files and clearly identified. This practice will facilitate identification of records stored on electronic media when it is time to migrate them.

Metadata

To effectively manage electronic records throughout their life cycle, it is critical that the metadata used to identify them is detailed and descriptive, providing information about the structure, content, and origin of information. These metadata requirements must be jointly established by both the originating program office and by the Records Management Division. With adequate metadata, records can be retrieved effectively and purged when no longer needed, without having to be printed out for records disposition purposes.

Electronic Recordkeeping Certification Program

The Records Officer's highest priority is to ensure that support for records management criteria is incorporated into requirements specifications and test plans of new information and knowledge management systems. The second highest priority is to review existing systems within the FBI to ensure compliance. Development efforts may continue on new information systems; however, it is incumbent on the Project Manager of any information or knowledge management system in development to ensure coordination with the Records Officer because the system may not become operational without the Records Officer's authorization. To ensure this, the FBI created the Electronic Recordkeeping Certification (ERKC) process. Implementation of the ERKC process ensures that the systems the FBI develops and maintains comply with statutory and agency electronic recordkeeping requirements. The ERKC process incorporates electronic recordkeeping requirements into the system development life cycle (SDLC) so that all system development activities can appropriately consider electronic recordkeeping issues from the earliest stages of acquisition and design. (See the FBI Electronic Recordkeeping Certification (ERKC) Manual for more detailed information.)

E-Files Purging

Copies of records are often maintained in electronic form, either on office shared drives, individual workstations, or portable magnetic or optical media (CDs, diskettes, tapes). Many of these records are word processing documents used to produce the recordkeeping or official copy of a record, and are kept for convenience of reference or reproduction. If these copies are created solely to produce a recordkeeping or convenience copy, they should periodically be deleted, once it is verified that the official or recordkeeping copy has been produced and appropriately filed. Electronic mail records residing on the 'live' system should be removed once the record is printed and filed or transferred to an appropriate recordkeeping system. Since many word processing and electronic mail copies reside on individuals' workstations (on H:/ drives, for example), or in individual electronic mail accounts, it is the responsibility of each employee to manage these files. Each employee who temporarily stores official records in any location should do the following:

- Follow the guidelines of this manual to determine the record status of documents stored on their home or locally shared drives
- Ensure an official recordkeeping copy of records they create or receive is placed in the appropriate file (paper or electronic)
- Participate in periodic e-records cleanout activities

4.2.2.8.2. Types of Electronic Records

Electronic Mail

Electronic Mail (e-mail) is a frequent means of communication within the FBI, and many e-mail messages are records. An e-mail message is a record if it contains information that is pertinent to an investigation, to an intelligence-gathering effort, to a significant administrative matter, or to other official FBI functions and the information is not duplicated in Bureau files. The creator or recipient of an e-mail communication must make a determination whether the message fits the definition of a record.

An e-mail message is probably a record if:

- The message documents agreements reached in meetings, telephone conversations, or other e-mail exchanges on substantive matters relating to FBI investigative or other activities.
- The message provides comments on or objections to the language in drafts of significant policy statements or action plans.
- The message supplements information in official files and it adds to a complete understanding of FBI operations and responsibilities.
- The recipient or its successor would need to reference this e-mail in the future in carrying out responsibilities.

When doubt exists about whether or not an e-mail is a record, it should be treated as a record and incorporated into Bureau files. E-mail records cannot be deleted from the e-mail system unless a copy has been incorporated into a paper-based or electronic recordkeeping system. E-mail communication systems (GroupWise, Outlook, etc.) are not recordkeeping systems. E-mails

(whether record or non-record) containing information pertinent to matters covered by current litigation, investigations, or special inquiries of any type may not be deleted until their use for these purposes is completed.

For more information, consult the guide When Are E-Mails Records?.

Databases (Electronic Information Systems)

The Bureau has automated many functions using electronic information systems. Records that were once kept in paper form now exist in a variety of digital formats. Many of the Bureau's information systems, or databases, contain Federal records. Information systems consist of the following components:

- **Inputs**: information entered into the system. This may be done by scanning paper documents, uploading from other information systems, manually keying in information, or other types of interfaces
- **Outputs**: records produced by system processing. These may take the form of reports, statistical summaries, data files uploaded to another system, or other types of regularly produced information products
- **Master files**: records maintained on the 'live' system. Also referred to as data files.
- **Documentation**: records about the system and software. These include user guides, data dictionaries, and file layouts
- **Recordkeeping standards and certification practices**: the Bureau has established guidelines for electronic records systems that can be found in the ERKC manual.

Web Sites

Most Federal agencies use web-based technologies to assist in carrying out their mission. They may use Web sites to disseminate information also available in other forms or to conduct on-line business activities. The Federal Records Act applies to all Federal agency records, including Web records. The E-Government Act of 2002 (Public Law 107-347) places a number of public site requirements on the Office of Management and Budget (OMB), NARA, and the agencies, in the areas of enterprise architecture, information access and security, and accessibility to persons with disabilities.

Web sites contain content records representing information presented on the web site and administrative records providing evidence of the management and operations of the web site. Many web sites contain online forums, bulletin boards, chat rooms, etc. Employees who use these electronic communication venues to reach agreements or to transmit messages on substantive matters relating to FBI investigative, intelligence or other activities should treat the exchange as a record. A copy should be printed and added to the related case file. Many FBI web pages contain organizational charts, publications, graphic presentations, interactive programs, and links to information repositories. The Records Disposition Unit (RDU) in conjunction with the ITOD has developed a disposition authority for the administrative records associated with the

FBI's public web site, www.fbi.gov. RDU also assists program offices with developing disposition authorities for records maintained on internal FBI web sites.

Imaged (Converted) Records

Sometimes records are created in one media or format, but copying them to another better meets the Bureau's business needs. Records in paper form may have more value if converted to a digital format; conversely, some records created electronically may be more useful if printed to paper. Some factors that may lead to a change in media are as follows:

- There is a legal requirement (NARA transfer, evidence in court)
- The current format or media is obsolete (records cannot be accessed by current technology)
- The current format or media is nonstandard and/or no longer supported by the manufacturer
- Another format would better meet business needs
- The current format or media is not supported by Bureau recordkeeping systems
- The most common change in format and media is from analog (paper documents, photographs) to digital.

Imaging is the process of converting analog (usually paper) documents to digital image files. These files are essentially a picture of the document that can be stored on magnetic or optical media. Images can be in a number of software-dependent formats, such as .gif (Graphical Interface File); .jpg. (Joint Photographic Expert Group); and .tif (Tagged Image File Format). In order to search and retrieve image files, some form of indexing information—or metadata—must also be recorded for each document. The index, or metadata, is typically maintained in a separate database linked to the image files.

Images can also be converted to searchable electronic text files through Optical Character Recognition (OCR) software that reads the scanned image and produces text based on recognized patterns. The resulting text can then be stored as word processing documents (such as Word or WordPerfect) and have full-text search capabilities.

The decision to convert records to imaged or OCR files should be based on an office's business needs balanced against the costs. Not all paper records are good candidates for imaging. Offices should consider the following factors before implementing an imaging project:

- Volume of records. Imaging is generally used for large volumes of records
- Access needs. Imaging may enhance operations when multiple and/or geographically diverse users need access
- Records disposition. Imaging is generally not used for records with very short retention periods
- Legal acceptability. If paper copies are needed for original signatures, other authentication measures, or forensic analysis

Advantages:

- High-density storage
- Quick retrieval time
- Access by multiple users
- Ease of adding and updating records
- Ease of copying
- File integrity (image files cannot be altered)

Disadvantages:

- Equipment costs
- Hardware and software dependence
- Indexing/metadata requirements
- Uncertain life expectancy of storage media
- Added security requirements if records shared on Local Area Network (LAN) or Wide Area Network (WAN)
- Migration and data conversion requirements

Recordkeeping Requirements for Imaged Records

Paper records that are converted to scanned images may not be automatically disposed. Before paper files are destroyed, RDU must examine the files to determine if they require disposition authority from NARA. In some cases, NARA and the Bureau may agree to transfer the paper files rather than the scanned images. Therefore, when converting paper files to scanned images, provisions must be made to keep the paper files in a searchable arrangement until disposition authority is received.

Evidence that is converted to digital format by the Document Conversion Laboratory (DocLab) should not be incorporated as a bulky or enclosure behind the file of the related investigative or intelligence case file. Rather, at the conclusion of the investigation, the scanned evidence contained on diskettes, CDs, DVDs, etc. should be returned to the contributor or destroyed by following the Rules of Evidence.

For large or priority scanning projects, contact the RMD Document Conversion Laboratory.

4.2.3. Retrieving Information from Bureau Records

4.2.3.1. Outside the Bureau

4.2.3.1.1. Freedom of Information Act (FOIA) and Privacy Act (PA)

The **Freedom of Information Act** is a Federal statute that provides any person a right of access, enforceable in court, to virtually every record in the possession of an agency unless that record is protected from disclosure by one or more of the FOIA's nine exemptions. **The Privacy Act of 1974** is a Federal statute that provides individuals with a right of access, enforceable in court, to

records pertaining to themselves unless those records are protected from disclosure by any of the Privacy Act's exemptions.

RMD's FOIPA offices (Records/Information Dissemination Section) process requests received from a broad range of the general public, including private citizens, scholars, historians, members of the news media, prisoners, and current employees. These requests are processed according to the provisions of the FOIPA, Title 5, United States Code, Sections 552 and 552a. Identifiable material is reviewed line-by-line, and all nonexempt information is released. Information denied by one or more provisions of the Acts is identified and marked with the appropriate exemption(s).

Private citizens can make a request by submitting their complete name, current address, date and place of birth, and any additional information such as previous addresses, employment, alias, and other information as needed to http://FOIA.FBI.gov. Providing a daytime telephone number can also aid in responding to a request. A notarized signature or declaration pursuant to Title 28, United States Code, Section 1746 is also required. This procedure insures that any documents, if located, are released only to an individual having right to access.

All requesters have the right to appeal any denials of information. Appeals can be directed in writing to the Office of Information and Privacy, Department of Justice, within 60 days of the date of the release letter.

4.2.3.1.2. National Name Check Program (NNCP)

The National Name Check Program disseminates information from FBI files in response to name check requests received from Federal agencies and other law enforcement entities including internal FBI offices; components of the Legislative, Judicial and Executive branches; friendly foreign police and intelligence agencies; and state and local law enforcement agencies within the criminal justice system. Name checks are provided by the FBI to other government agencies under Executive Order 10450 ("...the appointment of each civilian officer or employee in any department or agency of the government shall be made subject to investigations.") The 1990 Appropriations Act authorized the FBI to establish and collect user fees from non-law enforcement agencies to offset the cost of providing name check services. The National Name Check Program is managed by RMD.

4.2.3.1.3. Mandatory Declassification Review

Executive Order (EO) 12958, Part 3, Section 3.5, as amended, sets forth provisions for Mandatory Declassification Review (MDR) of classified information by the originating agency upon request. Agencies conducting MDRs shall declassify all information that no longer meets the standards for classification under the EO. The agency shall then release the information to the requester unless withholding is authorized and warranted under applicable law. MDR requesters have the right to make administrative appeals to the Department Review Committee (DRC) and if dissatisfied with the ultimate DRC's decision, may appeal to the Interagency Security Classification Appeals Panel (ISCAP).

The EO states that any person may request an MDR. Declassified and unclassified information must be processed by the terms of the FOIPA for release to the requester. To access information,

a requester must give a reasonable description of the records sought to enable the agency perform a search with a reasonable effort. However, if the responsive records have been reviewed for declassification within the past two years of the date of the MDR request and/or are the subject of pending litigation, the requester must be informed of the denial of his request and advised of his/her appeal rights

The majority of MDR requests to the FBI originate with Presidential Libraries and/or NARA. Presidential Library records that are more than 25 years old are subject to MDR review according to the Presidential Libraries Act of 1955 (the Act). The Act mandates the dissemination of documents from Presidential Libraries established prior to 1978. Recommendations to withhold any declassified and/or unclassified information are made in accordance with the Act's 'Donor's Deed of Gift' provision. In 1978, Congress passed the Presidential Records Act (PRA) which changed the legal status of Presidential and Vice Presidential materials. Under the PRA, effective on January 20, 1981, post 1978 Presidential and Vice Presidential materials are eligible for access five years after a change of administration. The records of the Ronald W. Reagan administration were the first to be administered under the PRA.

4.2.3.1.4. Discovery

Access to FBI documents may be obtained in civil litigation through judicial processes such as subpoenas and discovery requests. Questions regarding such civil and criminal litigation matters should be addressed to the Office of the General Counsel. As a result of discovery or other access requests, the Bureau may place a disposition 'freeze' on particular categories of documents needed for litigation purposes. See Processes and Procedures: 3.4.1. Routine Freezes—Civil and Criminal Matters and 3.4.2. Expanded Freezes—Civil and Criminal Matters for more information on litigation freeze procedures for both routine and expanded discovery processes.

4.2.3.2. Internal Access to FBI Records: Informal Review of Personnel File

FBI employees who wish to inspect their Official Personnel File can review and comment on documents in the file, but may not remove them. They can submit a response or rebuttal to any document in the file. At the time of their annual performance rating, employees are permitted access to the performance folder which contains documentation related to them employee's performance rating.

An employee's field office personnel file copy can be made available for inspection within 15 days of a request, and the employee's FBIHQ personnel file within 45 days. Requests for copies must be made through a Freedom of Information Act request. Requests to view an OPF are made through an authorized person, and the files can be viewed at the field office or division where the employee is assigned.

Certain confidential information, including the background investigation, testing materials, and other sensitive information, may need to be reviewed and/or removed from an individual's OPF consistent with the Privacy Act of 1974 and classification regulations before access is permitted.

Each division is responsible for designating at least one individual to review OPFs before the employee's informal review.

To request an informal review of personnel files, the employee completes an FD 834, Request for Access to Official Personnel File, and gives it to the Division point of contact who handles information access. Upon approval, the OPF is sent to the Division point of contact who reviews it and removes any documents in accordance with regulation. The requesting employee may then review the file.

4.2.3.3. Storing, Transferring, and Retrieving FBI Records for Internal Use

4.2.3.3.1. Transferring Records

Headquarters offices may store records at the Alexandria Records Center. When transferring administrative records to the ARC, please note that only main files in Classifications 319 and 67Q are stored at the ARC. Subfiles in these Classifications are maintained by the originating division.

To transfer an individual case file to the ARC, with the exception of Personnel Records (See Processes and Procedures: 2.3.2.5. Transferring Records to the ARC), the transferring unit must ensure that a file has been opened as the first serial document by uploading it into ACS. The serial one should be addressed to the ARC in care of JEH, Room 1B204. DO NOT send ARC mail and files to the Interim Central Records Complex (ICRC) in Winchester, Virginia.

All subsequent case documents must be serialized before they are sent to the Records Center for filing in the case jacket. Any (case) documents received at the Records Center without a serial number are returned to the submitting office. Any transfer of one cubic foot or more of records to the ARC at any one time must be approved by RSMU before the transfer takes place. Please see instructions in the next section, Transferring Records to the ARC.
Field offices maintain both original files and copies of files. The original communications must be retained in the headquarters city and may not be charged out to or filed as a serial in duplicate files in the resident agency off site location (RA/OS). In extraordinary circumstances, serials in the original headquarters city file may be charged out and recharged on a case-by-case basis to personnel assigned to the RA/OS when it has been determined by the Squad Supervisor Resident Agent or Supervisory Special Agent (SSRA/SSA) that the serials are necessary and enhancing to conducting day-to-day business.

All original files, including those opened in the RA/OS, must indicate on the case records in ACS that the file is located at the RA/OS. This can be done by using the Squad field or the REMARKS field. All original files retained in the RA/OS must be maintained in accordance with FBI procedures in the Resident Agency headquarters city facility unless an RA/OS is in compliance with the requirements for storage of classified material. (See Open Storage Secure Area Checklist.)

Transferring Records to the ARC

To transfer large volumes of records to the ARC for storage, the following procedures must be followed:

The transferring unit must notify RMD (RSMU) by e-mail at least two weeks ahead of the intended shipping date, indicating the volume, classification, date span, and disposition (if

known) of the records. When RSMU receives a storage request, it is reviewed and determined if the records are appropriate for storage at the ARC.

If RSMU approves the storage, documents must be shipped to the ARC in the following manner:

- Records must be arranged and shipped in white, standard General Services Administration (GSA) boxes used throughout the Federal government for retiring records. These boxes can be obtained by contacting the RMCU Unit Chief at [redacted] Other boxes, including banker's boxes or Xerox boxes, cannot be accepted because they do not provide adequate protection for the records. b6 b7C
- If possible, all records in each box should have the same classification.
- Bulkies (oversized materials related to a case) should be included in the box with the corresponding case file. Do not put bulkies in separate boxes unless volume warrants.
- Identification information must be marked in black marker on each box. Mark the side of the box that states "Do not write on this side." DO NOT write any information on any other side of the box.
- On the outside of the box, the entire case number—including classification—must be listed. If more than one case is in a single box, indicate all case numbers.
- If more than one box is used for a case, the case number must be written on the box with the first serial number and the last serial number in the box. Continue marking boxes in this manner until all serials and bulkies for the case are included in boxes.
- If forms or records other than cases are being shipped, the form number or type of file must be indicated on the outside of the box.
- Each box must indicate the individual box number as well as the entire box count. For example, box 1 of 10; box 2 of 10, etc.

Create a list of the records being shipped. Include the name of the office, unit, section, and division that is storing the records; the name and telephone number of a point-of-contact; and a detailed and complete listing of the contents of each box. Make three copies of the list: put one in the first box of the shipment, send one to RSMU Alexandria Records Center, and keep one in the office as a reference. Also, send an electronic version of the inventory to the RSMU Unit Chief.

4.2.3.3.2. Environmental Standards/Preservation Requirements for Storing Records

All records, no matter what their media, are affected by the environment in which they are stored. Information recorded on paper is fairly stable and long-lasting, but even paper is vulnerable to harm from a variety of environmental hazards ranging from mold and mildew to fire or water. Non-textual records (such as audio recordings, computer tapes, photographs, and motion picture footage) are among the most fragile record forms. Adverse storage conditions hasten their deterioration and shorten their usability. Extremes in temperature and humidity as well as close contact with certain materials can cause detrimental physical and chemical reactions. Mishandling and abusive treatment can also cause damage to these special media formats,

causing loss of valuable information. Consequently, records stored on special media require environmental controls beyond those provided in the typical office environment.

Table 1 depicts the recommended temperature and humidity levels when storing non-textual records.

Table 1. Recommended Temperature and Humidity Levels for Non-textual Record Storage

Media	Temperature	Relative Humidity (RH)	Reference
Audiovisual formats (such as cassette, reel-to-reel, and video tapes, as well as photographic film)	Should not exceed 70° Fahrenheit	30-40% RH; do not exceed 50% RH	36 CFR §1232.26 (b)
Magnetic tapes (Nine track tapes and 3480 tape cartridges)	Between 62° to 68° Fahrenheit	35-45% RH	36 CFR §1234.30 (g) (2)
Optical (CDs/DVDs)	Between 39° and 68° Fahrenheit	20-50% RH	NIST

4.2.3.3.3. Storage for Electronic and Audiovisual Records

- Store magnetic media, including open-reel sound recordings and videocassettes, in containers made of polypropylene, polyethylene, or non-corrosive material.
- Store tapes, compact disks, and digital video disks vertically in jewel boxes or plastic containers that protect them from dust and debris.
- Store in secure areas that are protected against unauthorized access as well as from damage from fire, water, chemicals, insect infestation, or other potentially harmful conditions.
- Store away from magnetic fields, sources of vibration, and sunlight.
- Protect from contact with dust and dirt, whether present during use or in the storage area.
- Store vertically. Do not stack horizontally on shelves or leave unprotected on windowsills, desktops, or storage cabinets, or other areas of potential exposure to direct sunlight or other sources of heat.
- Prohibit eating, drinking, and smoking in special media storage areas.

For more detailed guidance on the maintenance of special media contact RMD or see the following:

- 44USC_3301_3314.doc for information on 36 CFR 1228.270 Electronic records, 36 CFR 1234.30 Selection and maintenance of electronic records storage media, 36 CFR 1234.32 Retention and disposition of electronic records, and 36 CFR 1234.34 Destruction of electronic records
- MIOG, Part 2, Section 35, ADPT Security Policy
- Part 1232 - Audiovisual Records Management from the www.nara.gov web site

4.2.3.3.4. Retrieving Records—Using the File Automated Control System (FACS) to request records from the ARC

To obtain access to FACS, the division computer specialist must request that ITOD add the user to the XREQUEST group in the FACS. Each Division, field office, and legat must have at least one person who has access to and can request files through FACS.

Once there is access to FACS, the user proceeds as follows:

- Sign-on to FBINET
- Select function key which corresponds to 'HQ File Automated Control'
- Select PF3 Request. The File Request screen appears. Type the following:

  a) FILE NUMBER

  b) REQUEST TYPE

  c) CHARGE TO – The official Bureau name (OBN) of the individual needing access to the file.

  d) SUBJECT – Indicate subject matter pertaining to file request.

  e) COMMENT – Add additional comments as needed. For example, if 1A Bulkies are needed, indicate this in the Comment field. If a file is urgently needed, also indicate that in this field.

After all the information is entered, submit the request by pressing the Enter key.

Requests for files sent by e-mail or telephone will not be filled. If a file is urgently needed, a unit chief or above must send an e-mail request to the RSMU Unit Chief detailing the circumstances that necessitate an exception to the request policy.

Because of the sensitive nature of some material maintained by RMD, the Bureau's need-to-know policy, and the importance of continually tracking the files, it is imperative that files be requested in the name of the person who will be reviewing the file. To maintain security and control of FBI records, it is necessary that each employee adhere to the file request policy. Files may not be given to another individual unless a record of that transfer is recorded in FACS.

RSMU locates and pulls the requested file and scans file identification information into FACS to track the file. The person requesting files is held responsible for the files until they are returned to RSMU. All files must be returned within 60 days of receipt or RSMU contacts the employee

after 60 days. When the files are returned to RSMU, the information is rescanned into FACS with a note that the file has been returned. It is then returned to storage.

4.3. Records Disposition

4.3.1. Records Scheduling

RDU assists FBI program managers with the review of new and existing records systems in order to evaluate and develop appropriate retention periods. This review or 'scheduling' is the process of developing mandatory instructions for what to do with records (and non-record materials) that are no longer needed for current government business. In addition to working with program managers, RDU also consults with the OGC, ITOD, the Office of Congressional Affairs (OCA), and other stakeholders who have an interest in the retention of the records. Following internal review, RDU prepares and submits to NARA a request for records disposition authority on a Standard Form 115 (SF 115).

NARA reviews the proposed disposition authority, works through RDU to answer any questions, prepares a written appraisal of the proposed request, and publishes a notice of the proposed disposition authority in the Federal Register. Following a comment period and barring any concerns about the proposed retention periods, the proposal is submitted to the Archivist of the United States for signature. Upon signature, the disposition authority becomes a legal agreement between NARA and the FBI on the length of time the records will be retained.

4.3.2. The FBI's Retention Plan

Approved disposition authorities are compiled into a set of instructions for managing records. At the FBI, this compilation is called the Records Retention Plan (the Plan).

The Plan provides instructions for the retention, disposal, or transfer of FBI records. It is broken down by records series (i.e., file classification) or for electronic records by system name. For each classification or system, the Plan includes a brief description of the records, a breakdown of the types of records covered by the classification number or system, and disposition instructions for each.

4.3.3. Applying the FBI's Disposition Authorities

The FBI's disposition authorities provide specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a prescribed period of time has elapsed. Other records are transferred to NARA a certain number of years after a case has closed. See [redacted] for a listing of Approved Disposition Authorities. b7E

4.3.3.1. Destruction of Administrative Records – Classifications 319 and 67Q

Most of the Bureau's administrative records have temporary retention periods. This means that after a certain period of time has elapsed, the records can be destroyed. As stated previously, administrative records relate to budget, time and attendance, supply, and other housekeeping functions common to all Federal government offices.

To facilitate destruction, administrative records should be closed or 'cut-off' at regular intervals, normally at the close of a fiscal or calendar year. This cut-off permits the segregation of a year's accumulation of related records in a discrete block. At the end of a specified time period, all records in that block can be destroyed, barring any record holds, freezes, or other actions that would temporarily extend the retention period.

4.3.3.2. Destruction of Investigative and Intelligence Records

The destruction of all investigative and intelligence-related records is directly managed by RDU, to ensure that the complex disposition requirements for these records are accurately and consistently applied. Offices should retain these classes of records until RDU issues guidance providing specific disposition instructions or directs the transfer of records in a certain classification number to FBIHQ for processing.

4.3.3.3. Disposition of Evidence

According to the Rules of Evidence, once a case is closed and all investigative needs have been exhausted, non-FBI generated evidence is returned to the owner/contributor, destroyed, or forfeited. The method of disposition depends upon the investigative case and the type of evidence, (i.e., contraband evidence is destroyed). Any evidence that has been scanned by DocLab and placed on a CD-ROM to aid in searching should be destroyed following case closure. Evidence that is FBI-generated, such as chain of custody forms, crime scene photographs, and laboratory analysis, should be filed in the related investigative case file and assume the retention period established for that file.

4.3.3.4. Disposition of Non-record Materials

Offices routinely print out reference copies of ECs, e-mail messages, and other documents. They also maintain electronic versions of the same documents on their e-mail communication and word processing systems. Offices accumulate reference materials, such as periodicals, vendor catalogs, newspaper articles, reports, and Federal Register notices. All of these non-record materials can be destroyed when no longer needed for reference purposes.

Offices should review non-record materials yearly, and destroy any materials that have been superseded or are no longer useful.

4.3.3.5. Disposition of Personal Files

Personal files are those materials that belong to an individual, not the FBI. Certain files are clearly personal (private), such as those that are not used in the transaction of FBI business. Personal files may contain references to or comments on FBI business, but they are considered personal if they are not used in the conduct of business.

Personal files include materials relating to political activities, personal and family matters, or social or civic activities or materials that are indirectly related to FBI business but outside the scope of the definition of Federal records. For example, diaries, notes, and calendars are considered personal if they are not prepared, received, or used in the process of transacting Bureau business.

Personal files should be clearly designated as such and should always be maintained separately from official FBI files. These materials can be destroyed or removed from the FBI when no longer required for personal reference.

4.3.3.6. Unauthorized Destruction of FBI Records

Bureau employees are responsible for preventing the unauthorized destruction, damage, or alienation of records. Records may not be destroyed or removed from the legal custody of the Bureau except in accordance with authorized dispositions. Any unauthorized destruction should be reported to RMD to initiate the necessary reports to the Director and NARA. Unauthorized destruction of Federal records can result in criminal penalties.

- Criminal Penalties

  The maximum penalty for the willful and unlawful destruction, damage, or alienation of Federal records is a $2,000 fine, three years in prison, or both (18 U.S.C. 2071).

- Reporting

  The Director reports any unlawful or accidental destruction, damage, or alienation of records to NARA. The report includes a complete description of the records with volume and dates if known; a statement of the exact circumstances surrounding the destruction, damage, or alteration of the records; a statement of the safeguards established to prevent further loss of documentation; and when appropriate, details of the actions taken to salvage, retrieve, or reconstruct the records.

  If necessary, the Archivist of the United States will assist the Director in contacting the Attorney General for the recovery of any unlawfully removed records.

4.3.3.7. Orphaned Records

Orphaned records are defined as those records that are left behind by their creators or owners. Orphaned records are sometimes abandoned in offices after the personnel have moved. FBI employees should be aware of their responsibilities in ensuring that records in their custody are not inadvertently left behind during office moves.

Initial review of orphaned records:

- Keep all files, binders, folders, photographs, tapes, diskettes, CDs, etc., in the same box or filing cabinet and in the same original order.
- Look through the files to obtain names, organizations, telephone numbers, or any other information that might help identify the owner or someone familiar with the files.
- Do not disassemble any of the files.
- Try to determine what the files are; if they contain any security classified materials; if the materials relate to a particular case or investigation; if they appear to be copies; and what the dates of the files are.

- Put a sheet of paper in the box or on front of the file cabinet indicating that you are trying to determine to whom these materials belong. Include your name and phone number so office occupants can contact you if there are any questions.

Continuing Research:

- Owner: Contact any individuals whose names appear in the files. If no personal names are present, but a unit/section/division name is present, check the FBI Intranet for contact information and call the supervisor of that unit/section/division. If an owner is located, arrange to transfer the records to that office. Document the transfer in an EC or e-mail message.
- ECs: Search for any ECs in the files. Search ACS to see if the EC has been uploaded.
- Administrative records: Check if the records are administrative in nature. Check the list of Classification 319 and 67Q disposition authorities to see if a description for a 319 or 67Q records series is similar to the material that you've located in the orphan files. If so, apply that 319 and 67Q disposition instruction.
- Supplies: Check if there are supplies or other non-textual materials in the box/cabinet. These are not records. Remove them and place them in a supply cabinet.
- Evidence: Check if there are photographs or other items that have been marked 'evidence'. Try to determine which case the evidence is associated with. If possible, contact that office to see if you can return it to them. As a last resort, contact the Evidence Program Office at the Laboratory for more information.
- Personal information: Check if the records contain personal information about an employee(s). If so, return the records to the supervisor of the unit to which the employee(s) reports. For example, T&A records should be returned to the appropriate unit to which they belong.
- Personal belongings: Check if the box/filing cabinet contains personal belongings. If possible, contact the individual to which the materials belong and arrange to return the belongings.
- Maps and drawings: Check if the files contain commercially available maps or illustrations, then they can be destroyed unless an owner is discovered.
- Binders and other Presentation Material: Check if there are multiple copies of binders, training brochures, PowerPoint slide handouts, etc. As long as one copy is made part of the official record, the other copies can be destroyed.
- Magnetic media: Check if there are diskettes, CDs, and other non-textual formats in the box/filing cabinet. Determine what is contained on these devices. If the material is a duplicate of records that are captured elsewhere in the official files, then these magnetic devices can be destroyed.

If any records relating to a major case such as PentaBomb are abandoned, please contact RMD immediately.

4.3.4. Identifying Records in Litigation

In certain circumstances, the FBI must deviate from normal disposition activities. This deviation can result in extending the retention period of records for a longer time or in destroying records earlier than prescribed by the disposition authorities. For the most part, these exceptions apply only to specified documents or files and not to the entire file classification. Record holds or freezes are typically imposed when there is a pending legal action or when records are required to support a re-opened investigation. Whenever record holds or freezes are initiated, all regularly scheduled destruction and/or transfer activities are suspended until resolution of the litigation or investigation.

Bureau employees must ensure that records needed for pending litigation, criminal prosecution and appeals, and inquiries and inspections are identified and protected from destruction or deletion until all legal and official uses are concluded. All previously-authorized destruction of FBI records in accordance with approved records disposition authorities is halted when there is a new legal or official need for the records. Identifying such records and marking them for retention is referred to as a freeze.

4.3.4.1. Routine Freezes—Civil and Criminal Matters

Routine freezes may be imposed whenever the OGC (for civil litigation) or a case agent (for prosecutions and appeals) receives notice of litigation potentially involving FBI records. The OGC's Civil Litigation Unit identifies relevant case file numbers for most civil litigation matters. RMD then publishes these numbers on the RDU Intranet web site. Offices and divisions must consult this Intranet site before undertaking any disposition activities to ensure that they will not inadvertently destroy documents related to the litigation. In most instances, offices will not need to search the manual indices for routine litigation freezes. Most civil lawsuits relate to relatively recent incidents and the manual indices generally pertain to matters more than several decades old. When it is necessary to search the manual indices of one or several field offices or headquarters divisions, OGC will notify the appropriate offices/divisions.

Freezes are not normally imposed for routine criminal prosecution purposes. Disposition instructions require that a case be closed for at least 10 years before any disposition action can take place, and an investigative file should not be closed until the prosecution and all appeals have been concluded.

An investigative file should not be closed until all appeals have been exhausted. Once the time for the standard appeal process has lapsed, the case agent should contact the United States Attorney's Office (USAO) to determine if an appeal has been filed. If an appeal has not been filed, the case may be closed. If an appeal has been filed and the USAO determines the FBI is to be involved, the case should remain open or be re-opened if it was closed. The case agent is responsible for making contact with the USAO every 180 days to determine the progress of the appeal. Once advised that all appeal issues have been resolved and no longer require FBI involvement, the case agent should draft a letter confirming this to the USAO, then request the case be closed.

4.3.4.2. Expanded Freezes—Civil and Criminal Matters

While routine freezes apply primarily to those records filed in Bureau recordkeeping systems such as ACS and BPMS, expanded freezes may apply to all documents, electronic files, electronic mail, or other materials of any type related to the identified subjects, including even copies and drafts of documents.

Expanded freezes may apply to both criminal and civil matters as well as to inquiries such as those from Congress or Inspectors General. They may be initiated by any field office, division, or OGC. Expanded freezes are often linked to the production of documents for discovery purposes. Most Equal Employment Opportunity (EEO) cases require expanded freezes because every piece of paper or word processing draft document relevant to the case must be produced, including copies in personal files as well as final approved versions in official files. In every case, both OGC (CDRU) and RMD should receive a copy of an expanded freeze notice to ensure that any cases identified for protection are listed on the RMD RDU Web site. See Litigation Freeze List on the Record Disposition Unit's Web site for a complete listing.

4.3.4.3. Records Holds - Re-opened Investigations

On occasion, cases that have been closed for many years are re-opened based on newly discovered evidence. In these instances, records liaisons in field offices should notify RDU of any renewed interest in a case. Upon notification, RDU will inform other offices of the renewed interest in the files. This will prevent the destruction of any records that might prove useful to the re-opened investigation.

4.3.5. Shortened Retention Periods: Expungements and Early Destructions

On occasion, RDU may remove or destroy certain documents or files prior to their authorized destruction or transfer date. Court orders may direct certain records to be expunged, and individuals may also request that certain records be expunged. Depending on the court order and the governing statute or program, expungement may mean the physical removal and destruction of some or all of the records, or it may mean the removal, sealing, and secure storage of records away from the remaining file. Most expungements are carried out according to one of the following statutes.

4.3.5.1. Federal Youth Corrections Act (FYCA)

Superseded By Policy Notice #0169N, titled "Expungement of FBI Records," dated 03/05/2009.

Effective Date: 03/05/2009.

4.3.5.2. Federal Pretrial Diversion Program

Superseded By Policy Notice #0169N, titled "Expungement of FBI Records," dated 03/05/2009.

Effective Date: 03/05/2009.

4.3.5.3. Presidential Pardons

Superseded By Policy Notice #0169N, titled "Expungement of FBI Records," dated 03/05/2009.

Effective Date: 03/05/2009.

4.3.5.4. Controlled Substances Act, 21 U.S.C § 844(b)(1) and (b)(2)

Superseded By Policy Notice #0169N, titled "Expungement of FBI Records," dated 03/05/2009.

Effective Date: 03/05/2009.

4.3.5.5. Privacy Act Expungements

Superseded By Policy Notice #0169N, titled "Expungement of FBI Records," dated 03/05/2009.

Effective Date: 03/05/2009.

4.3.5.6. Emergency Destruction of Records

Under certain conditions, records may be destroyed if they constitute a continuing menace to human health or to Bureau property. Records that have been exposed to radiological, biological or chemical agents, or that are otherwise contaminated or infested, should be reported to RMD immediately. Other circumstances that may warrant early destruction of records include wartime or other national emergency conditions. RMD will request approval for emergency destruction of the records from NARA. Upon concurrence from NARA, RMD will coordinate the appropriate means of destruction and generate a report describing the records and the circumstances of their destruction. See 36 CFR § 1228 Subpart F for more information on emergency destruction.

4.3.6. Identifying and Managing Historical Records

Almost every investigative and intelligence file classification contains some records that have been designated as permanent by NARA. Permanent records are those records that have been deemed sufficiently valuable to warrant continued preservation by the Federal government after their usefulness to the Bureau has expired. RDU works with NARA to identify these records and protect them as part of the historical documentation of the FBI's accomplishments. The Records Retention Plan identifies categories of permanent records and specifies at which point they are transferred to NARA. Permanent records include those case files related to investigations of the ten most wanted criminals, investigations of significant individuals, events and/or organizations, and those cases that evidence a precedent-setting program or otherwise constitute a landmark case.

4.3.7. Transfer of Permanent Records to NARA

RDU has sole responsibility for transferring records to NARA. All FBI divisions and offices must coordinate transfers through RDU.

Prior to the transfer of historical records to NARA, RDU and RIDS' Declassification Review Unit evaluate each file. The Declassification Review Unit checks each file to ensure that eligible information has been declassified. RDU reviews to locate Grand Jury, Income Tax, and Title III information. This privacy protected information is identified and marked so that it will be protected from release by NARA. During this final review, RDU de-indexes the records by

removing all references to these files from ACS and the manual indices, and updates the FACS with a notation that the file has been transferred to NARA. De-indexing and FACS updating prevent FBI users from searching fruitlessly for files that have been destroyed or transferred to NARA.

4.3.8. Transfer of Permanent Electronic Records

Although most Bureau electronic information systems do not yet have disposition authorities, some of the systems may contain permanent or potentially permanent electronic records. The transfer of electronic records is similar to the transfer of case files. RDU transfers the records, following disposition instructions, by submitting a Standard Form 258 to NARA. However, NARA has established some additional requirements for the transfer of electronic records:

- Records must be in a format and on a transfer media that is accepted by NARA at the time of transfer. See Expanding Acceptable Transfer Requirements: Transfer Instructions for Permanent Electronic Records and 36 CFR 1228.270 for NARA's detailed specifications for records transfer
- Records must include adequate documentation
- An NA Form 14097, Technical Description, or equivalent information must accompany the records

Appendix A: Legal Authorities

Several agencies, including the NARA, the Office of Management and Budget (OMB), and the General Services Administration (GSA) share oversight of records management in the Federal government. Listed below are brief descriptions of some of the relevant major statutes, regulations, and other laws, with links to the more detailed information:

- 36 CFR § 1220 through 1228: NARA regulations for Federal agency records management programs
- 44 USC § 3101 through 3107: Records management by Federal agencies
- 44 USC § 3301 through 3314: Disposal of records
- 44 USC § 3504 and 3513: Coordination of Federal Information Policy
- 44 USC § 3501 through 3520: Paperwork Reduction Act
- 18 USC § 2071: Criminal penalties for unauthorized disposal of Federal records
- OMB Circular A-130: Management of Federal information resources
- Management of Federal information resources
- FBI Records Retention Plan (NC1-65-82-04) and subsequent approved disposition authorities.

Records Management by Federal Agencies (44 U.S.C. Chapter 31)

Sec.

3101. Records management by agency heads; general duties
3102. Establishment of program of management
3103. Transfer of records to records centers
3104. Certifications and determinations on transferred records
3105. Safeguards
3106. Unlawful removal, destruction of records
3107. Authority of Comptroller General

§ 3101. Records management by agency heads; general duties

The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and 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.

§ 3102. Establishment of program of management

The head of each Federal agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. The program, among other things, shall provide for—

(1) effective controls over the creation and over the maintenance and use of records in the conduct of current business;

(2) cooperation with the Administrator of General Services and the Archivist 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 disposal of records of temporary value; and

(3) compliance with sections 2101-2117, 2501-2507, 2901-2909, and 3101-3107, of this title and the regulations issued under them.

§ 3103. Transfer of records to records centers

When the head of a Federal agency determines that such action may affect substantial economies or increased operating efficiency, he shall provide for the transfer of records to a records center maintained and operated by the Archivist, or, when approved by the Archivist, to a center maintained and operated by the head of the Federal agency.

§ 3104. Certifications and determinations on transferred records

An official of the Government who is authorized to certify to facts on the basis of records in his custody, may certify to facts on the basis of records that have been transferred by him or his predecessors to the Archivist, and may authorize the Archivist to certify to facts and to make administrative determinations on the basis of records transferred to the Archivist, notwithstanding any other law.

§ 3105. Safeguards

The head of each Federal agency shall establish safeguards against the removal or loss of records he determines to be necessary and required by regulations of the Archivist. Safeguards shall include making it known to officials and employees of the agency—

(1) that records in the custody of the agency are not to be alienated or destroyed except in accordance with sections 3301-3314 of this title, and

(2) the penalties provided by law for the unlawful removal or destruction of records

§ 3106. Unlawful removal, destruction of records

The head of each Federal agency shall notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, or destruction of records in the custody of the agency of which he is the head that shall come to his attention and with the assistance of the Archivist shall initiate action through the Attorney General for the recovery of records he knows or has reason to believe have been unlawfully removed from his agency, or from another Federal agency whose records have been transferred to his legal custody. In any case in which the head

of the agency does not initiate an action for such recovery or other redress within a reasonable period of time after being notified of any such unlawful action, the Archivist shall request the Attorney General to initiate such an action, and shall notify the Congress when such a request has been made.

§ 3107. Authority of Comptroller General

Chapters 21, 25, 27, 29, and 31 of this title do not limit the authority of the Comptroller General of the United States with respect to prescribing accounting systems, forms, and procedures, or lessen the responsibility of collecting and disbursing officers for rendition of their accounts for settlement by the General Accounting Office.

Disposal of Records (44 U.S.C. Chapter 33)

Sec.

§ 3301. Definition of records

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

§ 3302. Regulations covering lists of records for disposal, procedure for disposal, and standards for reproduction

The Archivist shall promulgate regulations, not inconsistent with this chapter, establishing—

(1) procedures for the compiling and submitting to him of lists and schedules of records proposed for disposal,

(2) procedures for the disposal of records authorized for disposal, and

(3) standards for the reproduction of records by photographic or microphotographic processes with a view to the disposal of the original records.

§ 3303. Lists and schedules of records to be submitted to the Archivist by head of each Government agency

The head of each agency of the United States Government shall submit to the Archivist, under regulations promulgated as provided by section 3302 of this title—

(1) lists of any records in the custody of the agency that have been photographed or microphotographed under the regulations and that, as a consequence, do not appear to have sufficient value to warrant their further preservation by the Government;

(2) lists of other records in the custody of the agency not needed by it in the transaction of its current business and that do not appear to have sufficient administrative, legal, research, or other value to warrant their further preservation by the Government; and

(3) schedules proposing the disposal after the lapse of specified periods of time of records of a specified form or character that either have accumulated in the custody of the agency or may accumulate after the submission of the schedules and apparently will not after the lapse of the period specified have sufficient administrative, legal, research, or other value to warrant their further preservation by the Government.

§ 3303a. Examination by Archivist of lists and schedules of records lacking preservation value; disposal of records

(a) The Archivist shall examine the lists and schedules submitted to him under section 3303 of this title. If the Archivist determines that any of the records listed in a list or schedule submitted to him do not, or will not after the lapse of the period specified, have sufficient administrative, legal, research, or other value to warrant their continued preservation by the Government, he may, after publication of notice in the Federal Register and an opportunity for interested persons to submit comment thereon—

(1) notify the agency to that effect, and

(2) empower the agency to dispose of those records in accordance with regulations promulgated under section 3302 of this title.

(b) Authorizations granted under lists and schedules submitted to the Archivist under section 3303 of this title, and schedules promulgated by the Archivist under subsection (d) of this section, shall be mandatory, subject to section 2909 of this title. As between an authorization granted

under lists and schedules submitted to the Archivist under section 3303 of this title and an authorization contained in a schedule promulgated under subsection (d) of this section, application of the authorization providing for the shorter retention period shall be required, subject to section 2909 of this title.

(c) The Archivist may request advice and counsel from the Committee on Rules and Administration of the Senate and the Committee on House Oversight of the House of Representatives with respect to the disposal of any particular records under this chapter whenever he considers that—

(1) those particular records may be of special interest to the Congress; or

(2) consultation with the Congress regarding the disposal of those particular records is in the public interest. However, this subsection does not require the Archivist to request such advice and counsel as a regular procedure in the general disposal of records under this chapter

(d) The Archivist shall promulgate schedules authorizing the disposal, after the lapse of specified periods of time, of records of a specified form or character common to several or all agencies if such records will not, at the end of the periods specified, have sufficient administrative, legal, research, or other value to warrant their further preservation by the United States Government. A Federal agency may request changes in such schedules for its records pursuant to section 2909 of this title.

(e) The Archivist may approve and effect the disposal of records that are in his legal custody, provided that records that had been in the custody of another existing agency may not be disposed of without the written consent of the head of the agency.

(f) The Archivist shall make an annual report to the Congress concerning the disposal of records under this chapter, including general descriptions of the types of records disposed of and such other information as he considers appropriate to keep the Congress fully informed regarding the disposal of records under this chapter.

§ 3308. Disposal of similar records where prior disposal was authorized

When it appears to the Archivist that an agency has in its custody, or is accumulating, records of the same form or character as those of the same agency previously authorized to be disposed of, he may empower the head of the agency to dispose of the records, after they have been in existence a specified period of time, in accordance with regulations promulgated under section 3302 of this title and without listing or scheduling them.

§ 3309. Preservation of claims of Government until settled in General Accounting Office; disposal authorized upon written approval of Comptroller General

Records pertaining to claims and demands by or against the Government of the United States or to accounts in which the Government of the United States is concerned, either as debtor or creditor, may not be disposed of by the head of an agency under authorization granted under this chapter, until the claims, demands, and accounts have been settled and adjusted in the General Accounting Office, except upon the written approval of the Comptroller General of the United States.

§ 3310. Disposal of records constituting menace to health, life, or property

When the Archivist and the head of the agency that has custody of them jointly determine that records in the custody of an agency of the United States Government are a continuing menace to human health or life or to property, the Archivist shall eliminate the menace immediately by any method he considers necessary. When records in the custody of the Archivist are disposed of under this section, the Archivist shall report their disposal to the agency from which they were transferred.

§ 3311. Destruction of records outside continental United States in time of war or when hostile action seems imminent; written report to Archivist

During a state of war between the United States and another nation, or when hostile action by a foreign power appears imminent, the head of an agency of the United States Government may authorize the destruction of records in his legal custody situated in a military or naval establishment, ship, or other depository outside the territorial limits of continental United States—

(1) the retention of which would be prejudicial to the interests of the United States, or

(2) which occupy space urgently needed for military purposes and are, in his opinion, without sufficient administrative, legal, research, or other value to warrant their continued preservation.

Within six months after their disposal, the official who directed the disposal shall submit a written report to the Archivist in which he shall describe the character of the records and state when and where he disposed of them.

§ 3312. Photographs or microphotographs of records considered as originals; certified reproductions admissible in evidence

Photographs or microphotographs of records made in compliance with regulations under section 3302 of this title shall have the same effect as the originals and shall be treated as originals for the purpose of their admissibility in evidence. Certified or authenticated reproductions of the photographs or microphotographs shall be admitted in evidence equally with the original photographs or microphotographs.

§ 3313. Moneys from sale of records payable into the Treasury

Money derived by agencies of the Government from the sale of records disposed of under this chapter shall be paid into the Treasury of the United States unless otherwise required by law.

§ 3314. Procedures for disposal of records exclusive

The procedures prescribed by this chapter are exclusive, and records of the United States Government may not be alienated or destroyed except under this chapter.

Appendix B: Sources of Additional Information

- Records Management Training is provided semi-annually at a designated location. (status pending)
- RMD website URL (intranet): [redacted] b7E
- NARA website URL (internet): http://www.archives.gov/
- OMB website URL (internet): http://www.whitehouse.gov/omb/
- Other resources on future RMD/PPU Web site

Appendix C: Contact Information

Records Management Division, FBIHQ, for RMD telephone numbers and organization information see organizational chart and assignment chart

The Records Management Division is available for assistance with any records management issues. Please contact the RMD Mailbox on the FBI intranet for further information.

Appendix D: Records Compliance Instructions and Checklists

Classification 319 and 67Q Checklist Instructions

1.1. A 'system of records' can be properly identified as drop files, file fronts and backs, accordion folders, or any other file containers in a systematic arrangement that provides for access to the files.

1.2. Good records management practices dictate that administrative files (i.e., Classification 319 and 67Q) should be segregated from program-related files (i.e., investigative or intelligence) because administrative files usually have a much shorter active life and retention period. Classification 319 and 67Q files should be separated from program files and placed in a separate file drawer or cabinet.

1.3. Each Classification 319 file container (file front/back, drop folder, accordion folder) should be identified with:

The Classification number, alpha, and item number: (319A1, 319T5)
The case file number: (319W-HQ-A1487697)
Or both

The title of the 319 category as it appears in the Classification 319 Guide:
319A1, Time and Attendance Registers
319T5, Transitory Files
319W-HQ-A1487697, Policy Development Working Files

The calendar year in which the files were created or received: (2005)

If additional volumes or sections are created during the year, they may be further identified by months covered: January – March 2005, April – June 2005.

1.4. Additional volumes or sections added during the year for a particular 319 category should have the same information as the first volume (see 1.3). In addition, they should be marked with the volume or section number. They may include an optional: break down by dates (see 1.3).

1.5. Main files are those files originally opened by RMD for each 319 category. Only files of Bureau-wide interest or significance should be filed in the main file. If the file is a main file, it should be sent for filing in RMD's RSMU (ARC Room 1210, HQ)

Subfiles have been created for each division, field office, and legat. Subfiles should be used for those records that are not disseminated widely (for example, Bureau-wide or to all Field Offices) and do not have significance beyond the Division, Field Office, or Legat.

2.1. The 319 file numbers should be displayed on both serialized and unserialized documents in case files. It is not necessary to display the file number on records in 319 categories that are never uploaded; in fact, these often do not have a case file number assigned. For example, 319A1, Time and Attendance Registers, do not have a case file number assigned since it is unlikely that these records would need to be uploaded and serialized.

The main file number must be displayed on documents in the following format:

319I-HQ-A1234567

The subfile number must be displayed on documents in the following format:

319I-HQ-A1234567-AL
319I-HQ-A1234567-RMD

2.2. The title field on documents for subfiles will have the title of the case first, followed by the office/division name and then the subject matter of the document. For example:

Office Administration
Buffalo Division
Night And Weekend Schedule

Office Administration
Records Management Division
Policy and Procedures Unit (PPU)
Emergency Wardens Contact List

2.3. A response (for example, covering a lead) to a document should be filed in the same main or subfile as the original. Responses should be uploaded into the file from which the correspondence originated, not in the responding office's subfile. For example, Baltimore FO responding to an EC from Finance Division should upload the response into the Finance Division subfile.

2.4. Offices should avoid unnecessary duplication of records. Working files or convenience copies should be clearly identified, segregated from record copies, and purged when no longer needed.

3.1. Not every administrative document needs to be uploaded in ACS. Documents that need to be disseminated outside of the division/office or need to be accessed by one or more divisions/offices can be uploaded. Documents that pertain only to the business of a particular office/squad/unit need not be uploaded. For example, an individual unit's Monthly Accomplishments Report does not need to be uploaded to ACS. Because the unit's report is a 'feeder report' to the unit's section and thereafter the division, it is not necessary for each unit's report to be disseminated outside its division. A better way for units to maintain files of this type is to keep a chronological paper file of the reports. Offices may also open a folder in the unit's shared drive for electronic versions. Similarly, internal meeting or committee files, including minutes and agendas, do not need to be uploaded to ACS.

The paper file is still the official file. The electronic version in ACS is used for ease of reference and dissemination. Whether the document is uploaded or serialized in ACS or not, all documents should be filed together in chronological order in the appropriate 319 paper file.

3.2. Documents serialized into ACS should be identified by the appropriate 319 case file number. Note that the case file number does not include the item number because ACS does not

accommodate item numbers in the case ID field. Main-File file numbers should appear as follows: 319W-HQ-A1487697 and subfiles as: 319W-HQ-A1487697-RMD.

3.3. Documents filed in 319 categories may not be filed in additional classifications. If necessary, they may be filed in an additional 319 category. For example: the Headquarters Contract Unit is responsible for filing original purchase orders and related documents in 319B4, Purchases Exceeding the Simplified Acquisition Threshold, whereas the program unit COTR may file a copy of the purchase order and related documents in 319B23, Contract Administration Matters.

3.4. The title of the document should be entered as it appears in the Classification 319 Guide:

319J-HQ-A1487574, Facility Management
319W-HQ-A1487697, Policy Development Working Files

4.1. Originators should upload into either the main or a subfile, whichever is appropriate, but not both.

4.2. Offices should have at least begun the process of converting to the use of classification 319 for administrative files. However, many offices' filing practices have included filing non-administrative (program-related or investigative) records in a 66F file. These do not belong in classification 319; instead, the office should determine the correct program-related classification. If a classification cannot be found that fits the records, notify RMD/RPAS/PPU or RMD/RPAS/RDU.

Managing Office Administrative Records Using Classification 319 and 67Q

Each office/squad/division is responsible for maintaining paper files of Classification 319 records created or received in their subfiles. Files that are created or received in a main file are to be sent to the RMD's RSMU for filing. Offices are also responsible for uploading into the Automated Case Support (ACS) system those documents that are appropriate for electronic dissemination.

Checklist for Managing Office Administrative Records Using Classification 319 and 67Q

Managing Paper 319 and 67Q s: Files		
1.1.	Is a system of records set up for Classification 319 and 67Q categories used by the office?	☐ Yes ☐ No
1.2.	Is the file drawer/cabinet or other storage area clearly identified with 'Classification 319 or 67Q ' and the calendar year?	☐ Yes ☐ No
1.3.	Is each file folder identified with: — the correct Classification 319 or 67Q alpha and item number, (i.e., 319A1) — the corresponding title, (i.e., Time and Attendance Registers) — the date span of the records, (i.e., 2005)	☐ Yes ☐ No
1.4.	If there are additional volumes or sections opened during the calendar year, are they identified with the information in Question 1.3., and marked Volume 2, etc. as appropriate?	☐ Yes ☐ No
1.5.	Is the file appropriately designated as a subfile?	☐ Yes ☐ No
1.6.	Are closed or cut-off files regularly segregated from active files?	☐ Yes ☐ No
1.7.	Are new volumes or sections opened at the beginning of each calendar year?	☐ Yes ☐ No
Managing Paper 319 and 67Q s: Documents		
2.1.	Are documents identified with the appropriate 319 or 67Q case file number or 319 alpha and item number?	☐ Yes ☐ No
2.2.	Are documents that have been uploaded to the Automated Case Support (ACS) system identified with the case file number and serial number?	☐ Yes ☐ No
2.3.	Do Classification 319 and 67Q documents have the correct title (if applicable)? Is the title displayed correctly in the document's title field?	☐ Yes ☐ No
2.4.	Are original paper copies of documents uploaded to another division's subfile sent to that division to be filed?	☐ Yes ☐ No
2.5.	Are non-record duplicates or working copies separated from the official files and regularly purged?	☐ Yes ☐ No

Managing Electronic 319s		
3.1.	Does the office upload documents to ACS when appropriate?	☐ Yes ☐ No
3.2.	Are uploaded documents identified with the correct 319 case file number(s)?	☐ Yes ☐ No
3.3.	Are uploaded documents identified only with the correct 319 case file number(s) and not filed in additional classifications?	☐ Yes ☐ No
3.4.	Do uploaded documents have the title in the correct format (corresponding to the document's case file number)?	☐ Yes ☐ No
3.5.	Are responses to 319 correspondence filed in the originator's main or subfile?	☐ Yes ☐ No
Additional considerations		
4.1.	Are documents filed in both the main and subfile?	☐ Yes ☐ No
4.2.	Are 66F files still being used instead of the appropriate 319, 67, or other category?	☐ Yes ☐ No

Appendix E: File Cutoff Examples

Security Risk Assessments Database

Systems Outputs: Reports and Statistics:

Cut off when superseded by next report or statistical update

DELETE/DESTROY 1 year after cutoff

Class	319O
Item	5
File	319O-HQ-A1487618 - Approved Forms: Main File RMD only
Description	One record copy of each form created by an agency with related instructions and documentation showing inception, scope, and purpose of form.
Disposition	Cut off when related form is discontinued, superseded, or canceled. Destroy 5 years after cutoff
Disp. authority	GRS 16, 3a

Appendix F: Detailed Sample File Plan

FILE PLAN			
1. Office: Gordon Point Field Office Squad 8	2. Phone: 303 555 1234	3. Rm. No.: 334	4. For FY: 2005
5. Prepared by: [redacted] File Supervisor	6. Approved by [redacted] FBI Records Officer		7. Date: 01/03/2005

b6
b7C

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
67G	No file number has been assigned.	Supervisor's Drop File		Supervisor's Office	DISPOSITION NOT AUTHORIZED
319A1	No file number has been assigned.	Time and Attendance Registers	Time cards and leave records	T&A box, Cubicle A	Destroy after GAO audit or when 6 years old, whichever is sooner.
319A2	319A-HQ-A1487479	Leave Accounting Listings	Creating agency copy, when maintained.	Squad 8 central files, sec 1	Destroy when 3 years old.

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
319B14	319B-HQ-A1487504	Requisition Matters	Requestor's copies of requisitions, requests for supplies and equipment, including ammunition.	Squad 8 central files, sec 1	Destroy 7 years after completion or cancellation of requisitions or after next inspection cycle, whichever is later.
319B	319B-HQ-1497704	Contract Administration Matters	Records maintained by COTRs related to routine oversight and administration of contract employees.	Squad 8 central files, sec 1	DISPOSITION NOT AUTHORIZED
319D2	319D-HQ-A1487520	Budget Submissions	Cost statements, spend plans, rough data and similar materials accumulated in the preparation of annual budget estimates.	Squad 8 central files, sec 1	Destroy when 6 years and 3 months old.
319H4	319H-HQ-A1487554	Travel Vouchers	Copies of records relating to reimbursing individuals, such as travel orders, per diem vouchers	Squad 8 central files, sec 1	Destroy when 6 years old.

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
319O1	No file number has been assigned.	Administrative Notices	Notices and other types of issuances related to routine administrative functions (e.g., payroll, procurement, personnel).	Squad 8 central files, sec 1	Destroy when superseded or obsolete.
319O23	319O-HQ-A1487659	Inspection Matters	copies of documents maintained for inspection purposes such as interrogatories and self-inspection checklists.	Squad 8 central files, sec 1	DISPOSAL NOT AUTHORIZED.
319Q2	319Q-HQ-A1487639	Classified Document Access requests	Requests and authorization for individuals to have access to classified files.	Squad 8 central files, sec 1	Destroy 2 years after authorization expires. DISPOSITION AUTHORITY: GRS 18, 6
319Q19	319Q-HQ-A1487655	Visitors Logs for All Other Areas (not maximum security)	Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas.	Active: in SCIF or sign-in area. Closed: Squad 8 central files, sec 1	Destroy 2 years after final entry or 2 years after date of document, as appropriate.

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
319T1	319T-HQ-A1487667	Office Administration	Records accumulated by individual offices that relate to the internal administration or housekeeping activities of the office rather than the functions for which the office exists.	Squad 8 central files, sec 1	Destroy when 2 years old.
319X2	319X-HQ-A1487701	Submission to Annual or Other Major Reports	Monthly, quarterly, and annual reports created by subordinate units and forwarded to other entities as input into the Annual Report or other major reports.	Squad 8 central files, sec 1	DISPOSAL NOT AUTHORIZED
319X6	319X-HQ-A1487705	Submissions to the Mission and Functional Statements	Program and field office input into the final version of the FBI's mission and function statements.	Squad 8 central files, sec 1	DISPOSAL NOT AUTHORIZED
319X15	319X-HQ-A1487714	Statistical Accomplishments	Reports on significant accomplishments to meet strategic goals and objectives.	Squad 8 central files, sec 1	DISPOSAL NOT AUTHORIZED

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
91	91-GP-C122345 (control file – for other file #s see Kent)	Bank Robberies	Banks robberies, larceny, burglary, and extortion	Squad 8 central files, sec 2 - 5	PERMANENT Do not destroy

Appendix G: Key Words

ACS: Automated Case Support system. A centralized case management system used by the Bureau to electronically file and disseminate case files. ACS is made up of three components:

ICM: Investigative Case Management, is used to open cases and to maintain cases, leads, and ticklers

ECF: Electronic Case File is used to maintain, track, and disseminate documents, by assigning unique serial numbers to each document

UNI: Universal Index is used to maintain searchable metadata related to cases filed in ACS

Active Records: Records necessary to conduct the current business of an office. Generally maintained in office space

Adequate and Proper Documentation: A record of the conduct of U.S. government business that is complete and accurate to the extent required to document the organization, function, policies, decisions, procedures, and essential transactions of the agency and that is 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

Administrative Records: Records related to budget, time and attendance, supply, and similar housekeeping (or facilitative) functions common to most offices, in contrast to mission- or program-related records. Many administrative records of the Bureau are described in Classifications 319 and 67Q.

Arrangement: The act or result of placing files in a particular order or sequence

Case Files: Records, regardless of media, documenting a specific action, event, person, place, project, or other matter. For example:

Investigative Case Files: Document matters related to violations of the laws of the United States, counterterrorism, and other program activities

Intelligence Case Files: Documentation that includes information and its analysis pertaining to intelligence matters

Administrative Case Files: Document specific matters related to facilitative functions, such as human resources, budget, or transportation

Control Files: Files established for the purpose of administering specific topics or programs

Central Records System: The Bureau's centralized system for maintaining official investigative, personnel, applicant, administrative, and general files. The system includes the files, indexes, and abstracts

Charge Outs: Cards or other indicators placed in files that record the removal of a record, the date of removal, and its location (example: FD 5a)

Chronological Files: Files arranged by date

Classification:

1. A category of investigative or administrative case files;
2. A designation of national security classification level;
3. In records management terminology, the process of determining the sequence or order in which to arrange documents

Classification 319: The classification covering many categories of administrative records, such as travel, time and attendance, and property management

Closed Files: A file on which action or investigation has been completed

Convenience and Technical Reference Files: Non-record materials kept solely for reference purposes. They may be information copies of correspondence or documents from other offices, copies of manuals, instructions, or publications. These materials should be clearly separated from records and periodically purged of superseded or 'no longer needed' materials. Examples include copies of statutes, instructions, or directives; catalogues; technical journals; phone directories, etc.

Control Files: Topic files relating to a particular classification number or violation, containing both administrative and investigative records. Files are related to investigative classification numbers established for the purpose of administering specific phases of an investigative matter

Correspondence: Letters, memorandums, notes, electronic mail, and any other form of addressed written communication sent and received

Cutoff: Breaking or ending files at regular intervals, usually at the close of the calendar year, to permit their disposal or transfer in complete blocks and to permit the establishment of new files. Case files are generally cut off at the end of the year in which the case is closed

Disposition: Actions taken regarding records no longer needed for current government business. These actions include transfer to storage facilities or Federal records centers, transfer of permanent records to NARA, and disposal of temporary records

Disposition Authority: Legal authority empowering agencies to transfer permanent records to NARA or to carry out the disposal of temporary records. Must be obtained from the Archivist of the United States, and also, for certain temporary records, from the Government Accountability Office (GAO)

Documentation: Records required to plan, develop, operate, maintain, and use electronic records and software

Electronic Information System: A system that contains and provides access to computerized records and other information

Electronic Mail (E-mail): The process or result of sending and receiving messages in electronic form by remote computer terminals

Electronic Recordkeeping System: An electronic information system that manages electronic records throughout their life cycle

Executive Correspondence Files: Outgoing correspondence and other documents proposed for the Director's signature, and incoming senior level executive correspondence from the Congress, the White House, or the Department of Justice. Outgoing records are to be forwarded to the RMD Executive Secretariat (ExecSec). Incoming congressional correspondence must be entered into the ExecSec control database before routing for response

Expungement: The physical removal and destruction of some or all of a record or, depending on the court order and the governing statute or program, the removal, sealing, and secure storage of records

Federal Records Act: Otherwise known as 44USC 3101; enacted in 1950. An Act that requires all Federal agencies to make and preserve records containing adequate and proper documentation of their organization, functions, policies, decisions, procedures, and essential transactions

File:

1. An accumulation of records or non-record materials arranged according to a plan;
2. A unit, such as a paper or electronic folder, containing records or non-record materials;
3. Storage equipment used to store records or non-record materials

File Plan: A plan designating the physical locations(s) at which files are to be maintained, the specific types of files to be maintained there, and the organizational element(s) having custodial responsibility. See Appendix F: Detailed Sample File Plan

Files Cleanout Day: A day set aside at the end of each calendar year that is dedicated to organizing office files and disposing of eligible unneeded electronic and paper files

Freedom of Information Act (FOIA): Otherwise known as 5 USC 552; enacted in 1966. An Act that provides citizens access to Federal records, except for those records that are protected from public disclosure by exemption or exclusion

Freeze: Special circumstances, such as a court order or investigation, that require a temporary extension of the approved retention period

Intelligence Files: These files include information and its analysis pertaining to information gathering

Medium/Media: The physical format of recorded information. Includes paper, optical disk, magnetic tape, film, and other materials on which information can be recorded

Metadata: Information about the structure, content, and origin of information. For example, the sender, recipient, date sent, and subject of an e-mail message

Non-record Materials: Government-owned documentary materials excluded from the legal definition of records or not meeting the requirements of that definition. Included are extra copies of documents kept solely for reference, stocks of publications or forms, and library or museum materials

Office of Origin (OO): The organizational unit that initiated creation of a record, and that is typically responsible for the record's maintenance

00 (Double Zero) Files: Files created for each classification number containing records on procedures, instructions, statutes and laws, and other policy matters specific to that classification number

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. These records are reviewed for declassification and transferred to NARA in approximately 25-year increments

Personal Papers: Documentary materials belonging to an individual that are not used to conduct business. Must be clearly designated as such and kept separate from records

Policy Files (1): Records that document high-level policies, decisions, or responsibilities of the Bureau. These records include correspondence, meeting and committee minutes and agendas, directives, and other records that reflect the direction of the Bureau and the dissemination of Bureau policies

Policy Files (2): Records that are part of individual classifications (00Files). These records are copies of applicable statutes, decisions, or other legal background material relevant to the classification number. These files are kept as part of an investigative case classification. These differ from (1) above in that they do not document the formulation of Bureau policies or decisions but rather provide background information in the form of already existing policy

Privacy Act: Otherwise known as 5 USC 552a; enacted in 1974. An Act that regulates the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies

Program Records: Records that document the unique, substantive functions of the Bureau, in contrast to administrative records. Also referred to as mission-related records

Recordkeeping Requirements: Statements in statutes, regulations, or agency directives or other issuances specifying which records are to be created or received and maintained by agency personnel

Recordkeeping System: A manual or automated system in which records are collected, organized, and categorized to facilitate their retrieval, use, and disposition

Records (Federal): All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. (44 USC 3301)

Records (Administrative): Records related to budget, time and attendance, supply, and similar housekeeping (or facilitative) functions common to most offices, in contrast to mission- or program-related records. Many administrative records of the Bureau are described in Classification 319 and 67Q

Records (Investigative Files): These case files are the most common type of records created in the Bureau. Specific recordkeeping requirements are tied to the files' classification number. General instructions on what records to include in an investigative case file can be found in the MAOP part 2, section 2-5.1

Records Life Cycle: The concept that records pass through several stages: creation, maintenance and use, and disposition

Records Management Application (RMA): A software application that automates records management functions and manages electronic records throughout their life cycle

Records Retention Plan: A document providing mandatory instructions for what to do with records (and non-record materials) no longer needed for current business. The Plan provides authority for the disposal of temporary records and the transfer of permanent records to NARA

Record Set: The official record copy of publications or issuances, in contrast to stock or distribution copies

Reference Files: Non-record materials used solely for reference

Retention Period: The period of time during which records must be kept before final disposition

Schedule: A records retention plan. Also, a document providing disposition authority for one or more series of records

Serial: Documentary materials placed in case files and numbered sequentially

Technical Reference Files: Non-record copies of regulations, publications, articles, or other materials that are needed for reference but are not part of an office's records

Temporary Records: Records approved by NARA for destruction, usually after a specified retention period

Topic Files: Records arranged according to their general information or topic content. These can be correspondence, forms, reports, or other materials. These records relate to a general program or administrative function, not to a specific case

Transfer: The process of moving records from one location to another, especially from office space to a storage facility, or from office or storage space to NARA for permanent preservation

Transitory Files: Records, usually correspondence, relating to matters of short-term interest

Working Files: Records that accumulate as part of a work process but that do not necessarily have a place in the case file or other official file. These records can be distinguished by several factors:

They are usually of short-term value; they may not have continuing value once the project or investigation is closed

They tend to be more voluminous and less organized than more formal records systems

They are more efficiently managed by segregation from the official files

Appendix H: Acronyms

.gif	Graphical Interface File
.jpg	Joint Photographic Group File
.tif	Tagged Image File
ACS	Automated Case Support
AFIS	Automated Fingerprint Identification System
AG	Attorney General
ANSI	American National Standards Institute
ARC	Alexandria Records Center
ARS	Additional Record Sheets
BPMS	Bureau Personnel Management System
CJIS	Criminal Justice Information Services
CMF	Criminal Master File
COTR	Contracting Office's Technical Representative
CSS	Card Scanning Services
DCI	Director of Central Intelligence
DOJ	Department of Justice
DPS	document processing sub-element
DRC	Department Review Committee
EC	Electronic Communication
ECF	Electronic Case File
EEO	Equal Employment Opportunity
EFF	Electronic File Folders
e-Forms	Electronic Forms
ELSUR	Electronic Surveillance
ELU	Employment Law Unit
e-mail	Electronic Mail
EO	Executive Order
ERKC	Electronic Recordkeeping Certification
ERS	ELSUR Records System
ExecSec	Executive Secretariat
FACS	File Automated Control System

FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINET	FBI Network
FD	Finance Division
FIDS	FBI Intelligence Information Report Dissémination System
FIMF	Fingerprint Image Master File
FIRS	Fingerprint Identification Records System
FOIA	Freedom of Information Act
FYCA	Federal Youth Corrections Act
GAO	Government Accountability Office
GSA	General Services Administration
IAFIS	Integrated Automated Fingerprint Identification System
ICM	Investigative Case Management
III	Interstate Identification Index
IIR	Intelligence Information Report
INSD	Inspection Division
ISCAP	Interagency Security Classification Appeals Panel
ITN	Identification Tasking and Networking
ITOD	Information Technology Operations Division
JCP	Joint Committee on Printing
LAN	Local Area Network
MDR	Mandatory Declassification Review
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
NNCPS	National Name Check Program Section
NPRC	National Personnel Records Center
OBN	Official Bureau Name
OCA	Office of Congressional Affairs
OCIO	Office of the Chief Information Officer
OCR	Optical Character Recognition

OGC	Office of General Counsel
OMB	Office of Management and Budget
OO	Office of Origin
OPF	Official Personnel File
OPR	Office of Professional Responsibility
PARS	Performance Appraisals Reports
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PRA	Presidential Records Act
QH	Query History
QR	Query Record
RA/OS	Resident Agency Off-site Location
RANR	Receiving Agency Notification Report
RAS	Records Automation Section
RCMU	Records Creation and Maintenance Unit
RCU	Records Compliance Unit
RDU	Records Disposition Unit
RIDS	Records / Information Dissemination Section
RM	Records Management
RMA	Records Management Application
RMD	Records Management Division
RPAS	Records Policy and Administration Section
RSMU	Records Storage and Maintenance Unit
SA	Special Agent
SAC	Special Agent in Charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDLC	System Development Life Cycle
SSA	Supervisory Special Agent
SSRA	Squad Supervisor Resident Agent
the Act	Presidential Libraries Act of 1955
the Plan	Records Retention Plan
TPS	ten-print processing sub-element

TS/SCI	Top Secret / Sensitive Compartmented Information
UCFN	Universal Case File Number
UF	User Fee
ULF	Unsolved Latent File
UNI	Universal Index
USAO	United States Attorney's Office
WAN	Wide Area Network