This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault

The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **http://www.theblackvault.com**

U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

January 18, 2018

MR. JOHN GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384

FOIPA Request No.: 1381833-000
Subject: Most Recent version of the Records Management Manual

Dear Mr. Greenewald:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 69 pages of previously processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Please be advised that additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your information needs for this request, you may request an additional search for records. Submit your request by mail or fax to – Work Process Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely,

David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

U.S. Department of Justice
Federal Bureau of Investigation
Records Management Division

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-29-2015 BY J89J28T90 NSICG

RECORDS MANAGEMENT

USER MANUAL

May 2015

TABLE OF CONTENTS

1. Introduction

The Records Management User Manual (RM User Manual) provides a detailed explanation of records management procedures. It is a reference tool designed to supplement the Records Management Policy Implementation Guide (RM PG). Many policies and procedures which were introduced in the RM PG are more fully explained here.

The RM User Manual provides practical guidance for personnel responsible for applying and maintaining proper records management practices to all records, regardless of medium or format. While the RM User Manual contains links to relevant Sentinel Quick Guides and provides guidance on certain records management issues in relation to Sentinel, it is not a comprehensive guide to Sentinel; nor is it intended to replace the guidance set forth on the Sentinel website. Questions concerning Sentinel should continue to be submitted through the Sentinel Online Support application found under the Sentinel Help tab. The Indexing User Manual for Sentinel should be consulted for any indexing questions.

2. Records Compliance

The creation and maintenance of records is a vital part of Federal Bureau of Investigation (FBI) personnel's responsibilities and functions. The importance of proper records management is codified and emphasized throughout federal laws and regulations. The FBI reinforces these laws and regulations through policies and procedures which assign records responsibilities to FBI personnel. See RM PG, Section 2.8.

2.1. Records Reviews

To ensure FBI files are managed effectively, the Records Management Division's (RMD) Policy, Analysis, and Compliance Unit (PACU) conducts monthly records reviews by analyzing pending and closed records for policy compliance and provides each division, field office, and legal attaché (LEGAT) (together, "divisions and offices") with constructive feedback. See RM PG, Section 2.2.3. Divisions and offices are required to respond to each records review and complete corrective actions which will facilitate the efficient retrieval and sharing of information in support of the FBI's operational mission.

2.2. Additional Records Reviews

One example of an additional records review conducted by PACU is the missing entity (index) records review. PACU completes monthly reviews to assess whether at least one entity record has been created for each case opened during the previous month. Divisions and offices are required to respond to the missing entity records review and complete corrective actions identified. The Indexing User Manual for Sentinel should be consulted for information about the proper indexing of records.

3. File Plan

For records maintained in paper format or in electronic form in a shared directory within a division or office, folders must be arranged in an organizational schema, termed a file plan. A file plan is a listing in outline form of the main file headings and subfile headings for each record series and information system in an office. The plan shows every classification number or records series maintained by the office, regardless of the record's storage location. The plan identifies records in all media, including paper, electronic, and audiovisual, physically stored in the office; electronic records, whether on a local or remote computer server or on removable media such as CDs; records on other non-paper media such as digital video discs (DVD), audiotapes, and film; and records stored in other office file storage areas. Records described on the plan should include not only those originated in the office, but also any others received or otherwise acquired and used in the course of business.

The file plan lists the folders in the paper files or on the electronic shared drive or other repository and the calendar or fiscal year associated with the creation of each one. The FBI's file classification system should be used for folder names. For administrative records (such as travel vouchers), each year, in accordance with the relevant retention schedule, the previous year's folder should be closed and moved to inactive storage. If the subject matter continues to be needed in the filing system, a new folder is opened for the current year. This periodic cutoff process may be established at other than annual intervals (e.g., biannually) so long as it is an established chronological period and regularly completed. See Section 4 for an explanation of file cutoffs.

The file plan for each shared directory or records storage location is posted as the first file of the shared drive or records storage location, and must be available for inspection for records audit purposes. The file plan can be posted on the shared drive by creating a folder entitled "File Plan" and saving the document into the folder. File plans should be reviewed annually and updated as needed.

In Sentinel, the file plan is managed through a records management application (RMA) in compliance with records management policy.

See Appendix A for sample file plans for paper and electronic records.

4. File Cutoff

The point when files change from pending to closed, or active to inactive, is referred to as a file cutoff. File cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff, not with the creation or receipt of the records.

The record's purpose, use, and arrangement determine the file cutoff procedures. Most file cutoffs are determined either by date or by occurrence of an event or action. For some files, an event, such as completion of a project or discontinuance 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 and are cutoff based on the calendar or fiscal year.

4.1. Block Closed Records

All federal records have, or will have, disposition authority from the National Archives and Records Administration (NARA). In simple terms, this means all FBI records will be retained for a period of time and then they will either be destroyed or transferred to NARA for permanent storage. The length of time the records must be kept before either transferring or destroying them begins at the point of the file cutoff. For example, travel vouchers have a set retention period. Following the established cut-off procedures for removing each year's file accumulation to inactive storage will make it easier to determine when a block of records has reached a set date and may be destroyed. Similarly, if files closed during a particular year are systematically removed and kept together by year, it is simpler to identify them for destruction or transfer to NARA.

4.2. Implementing a File Cutoff

Sentinel electronically maintains the majority of investigative and administrative records created during the course of day to day business. Sentinel automates the functions of tracking, implementing, and maintaining file cut-offs and retention. Sentinel automatically recognizes when a cut-off action is applied and begins the retention clock for a particular record. Sentinel flags when the retention for a particular record or range of records has been met and requests approval to apply the disposition.

There are records, such as the Supervisor Drop File (66Q44), which for various reasons are not maintained in Sentinel. Those records, as well as the legacy administrative Classification 66 and pre-Sentinel hard copy case files, have cut-offs implemented as described in the following sections.

As set forth in section 4.8.10.1.4 of the RM PG, records and non-records relevant to a pending or reasonably anticipated matter in litigation or other proceeding, including criminal investigations, prosecutions, and appeals, and other inquiries, investigations and inspections, must be protected from destruction or deletion, even as an exception to standard records disposition practices and schedules, until all legal and official uses are concluded and personnel receive written confirmation from the OGC the

identification and protection of such information is no longer necessary. The Legal Hold Policy Directive 0619D contains further information on when legal holds may be issued, and the roles and responsibilities of FBI personnel and others with regard to a legal hold.

4.2.1. Ongoing Files (non-event driven)

Administrative records are an example of records which are cutoff by a non-event.

The retention period for most administrative records is contained in the Classification 319 Guide. The classification number and alpha character are written on the outside of the file jacket or folder, the file is titled as it appears in the Classification 319 Guide, and the calendar or fiscal year is noted. All appropriate material is placed in the file until the year's last calendar day. For digital files maintained on shared drives, if the actual classification number from the file plan is not being used to identify the contents of the shared drive folder, then the file plan should note which shared drive folder contains which records category / classification of records.

If a paper volume becomes too bulky before the end of the calendar year, a new volume identified with the same information is created, and labeled with the next sequential volume number (e.g., volume 2, 3, 4). On January 1 of the following year, the previous year's volumes are closed out and moved to inactive storage. A new file is created with the new calendar year noted. The new file series begins with volume 1 and new volumes are opened, as needed, in sequential order.

Based on office needs, closed files are stored in a closed files storage area, or elsewhere in the office, as long as the records are properly identified. The closed date is used to determine the time remaining before the records are eligible for destruction. For example, if the retention period is "DESTROY WHEN ONE YEAR OLD," the records are destroyed at the beginning of the next calendar year. In this case, "ELIGIBLE FOR DESTRUCTION 1/1/20xx" is written on all closed volumes.

This cutoff cycle is continued every January with the start of a new file series and closing of the previous year's file series. Each year, offices will review their hard copy closed files to determine if any are eligible for destruction. Offices will then destroy eligible paper files and / or files contained on shared drives.

4.2.2. Event-driven or Contingent Files

Records closed after a certain event or action are handled differently than records which are ongoing and have non-event driven disposition. For example, the disposition instructions for 319B, Contract Appeals, are "destroy one year after final action on decision." In this example, on the day the final action is made, the case is closed. 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 record types, follow these procedures:

- Identify folders as above

- During the calendar year, as a case is closed, mark "closed" on the folder or file front
- At the end of each calendar year, remove all cases closed during the year and maintain all closed cases from the 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

4.2.3. Unscheduled Administrative Files

Some administrative records do not have authorized retention periods, (e.g., Classification 319 Guide at 319J Item 12, Occupational Safety and Health Matters), which means they must be retained. For these records, establish yearly cutoffs and mark file covers with "DISPOSAL NOT AUTHORIZED."

4.2.4. 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 are needed for current business for only a year or two, and then become inactive. These data files are moved to inactive storage, offline, or near line for the remainder of their retention period. In some instances the information system includes a history file to which inactive records are moved. Other data files contain records needed on an ongoing basis.

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

The RMD's Records Automation Section (RAS), Records Management Application Unit (RMAU) can assist with any questions regarding this process.

4.3. File Cutoff Example: Classification 319O - Administrative Management Records

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
Disposition authority	GRS 16, 3a

5. Case Management

5.1. Case File Types

The majority of the FBI's mission-related or program records are arranged in case files related to a specific type of investigation or intelligence matter. Each case is assigned a file number, which consists of a file classification number indicating the general category of the case, an alpha designator for subcategories within the classification, a two-letter designation for the Office of Origin (OO), and a case number automatically created and assigned sequentially by the central recordkeeping system (currently Sentinel). An example of a file number is 91A-BA-1234576. A complete list of file classifications is contained on the FBI's Resource Planning Office website.

There are several types of investigative and non-investigative files used within the FBI. Investigative files include [redacted] preliminary investigations, full investigations, full enterprise investigations, positive foreign intelligence full investigations, spin off investigations, and unaddressed work. Non-investigative files include zero files, double zero files, administrative files, and control files. Administrative files are discussed in Section 6, the rest are discussed below. b7E

Appendix J of the Domestic Investigations and Operations Guide 0667DPG contains detailed guidance regarding the investigative management of these types of files, as well as the type of documentation required to be maintained within each file. The information is not repeated here. Additional, recordkeeping guidance follows.

5.1.1. Control "C" Files

Control "C" files are, in most instances, non-transitory records with a permanent retention and will be transferred to NARA. The title of the control file is indexed as a main record and all other matters are indexed as references.

5.1.2. Zero "0" Files

Zero files [redacted] through the same procedures [redacted] Zero files should be opened only when the office has miscellaneous documents which do not rise to the level of opening a case file. They are opened under main classifications [redacted]

5.1.2.1. Additional Guidelines for handling Zero files [redacted] b7E

Indexing Zero files: [redacted]

Serializing to a Zero file: If a document, including non-transitory record e-mail, does not relate to a specific FBI case, the document should be filed in the appropriate classification's Zero file, [redacted]

[redacted] b7E

Zero file 1As: If a 1A (FD-340) envelope contains records suitable for retention in a Zero paper file, the 1A envelope is filed directly beneath the responsive paper serial. [redacted] b7E

[redacted] Questions about whether a particular document must be retained in hard copy should be referred to your Chief Division Counsel or the Office of the General Counsel's (OGC) Investigative Law Unit.

Opening a Zero file for a new classification: In Sentinel, with the exception of the 319 and 67 classifications, each office may open a Zero file for each new classification. [redacted] b7E

5.1.3. Double Zero "00" Files

Double zero "00" files used to be opened for every classification except Classification 319, 67Q, and the 800 series. Double zero files are no longer being utilized or opened for new classifications.

5.1.4. Unaddressed Work Files

[redacted] b7E

The FD-71 and an Assessment file provide a mechanism to assign an Assessment to an Unaddressed Work file. In the FD-71, the Supervisor must select a reason for assigning the matter to the Unaddressed Work file and choose the appropriate classification. Upon serializing the FD-71, a new Unaddressed Work file will be opened. Guardian (FD-71a) does not have an "Unaddressed Work" option because Guardian leads cannot be placed in an Unaddressed Work status. See Appendix J, Section J.1.4.5.4, of the Domestic Investigations and Operations Guide 0667DPG for additional information.

5.2. File Jackets

Paper file jackets vary according to file content. Divisions and offices file fronts and backs are white with color-coded borders to enhance security and to facilitate sorting and routing.

Listed below are the colors located on file jacket borders:

- **BLACK (form 4-596)** - used for FBIHQ investigative and administrative files b7E
- **YELLOW (form 4-596a)** - used for files concerning [redacted]
- **BROWN (form FD-245.1)** - used for field office criminal investigative and administrative files
- **GREEN (form FD-245A)** - used for field office [redacted] (medium green, form 245A)
- **BLUE (form FD-245b.1)** - used for all LEGAT office files
- **RED (form FD-245c.1)** - used for field office [redacted] investigative files
- **SOLID WHITE (form FD-245d)** - once used for field office unofficial personnel files; no longer in use
- **PURPLE (form FD-245d.1)** - used for medical records related to field office personnel
- **ORANGE (form FD-245d.2)** - used for security records related to field office personnel

5.3. Universal Case File Number (UCFN)

Each case is assigned a universal case file number (UCFN). The case file number used for Sentinel is a universal number, assigned sequentially by the computer program.

Prior to 1991, each office (office of origin and auxiliary offices) 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. In April 1991, the FBI converted to a system whereby only one file number was used for each case, and the number was owned by the office primarily responsible for the case. An example of a UCFN format is 91A-BA-1234567.

[redacted] b7E

5.4. Encrypted and Password Protected Files in Sentinel

Documents imported into Sentinel should not be encrypted or password protected. If needed, and when appropriate, access to a case may be restricted or prohibited in Sentinel.

[redacted] b7E

5.5. Serializing

Each document placed in an investigative case file must be numbered in sequence. The individual documents included in each case file are referred to as serials; they are assigned sequential numbers as they are added to the file. Documents appropriate to serialize in the case file must meet the following criteria:

- They meet the definition of a federal record
- They contain information pertaining to the specific case or administrative file
- They are unique; not a duplicate of records already serialized in the case file (however, if a duplicate copy has substantive notes, thus rendering it a separate, original record, it must be serialized in the case file)

Sentinel performs this function automatically as information is imported or created within the central recordkeeping system.

5.6. Subfiles

Subfiles are separate files established under a main file to facilitate the efficient retrieval of pertinent information. They aid in the organization and administration of a substantive case which has become voluminous or complex. Subfiles are established on a case-by-case basis and are opened as the need arises. Supervisory approval is necessary and should be obtained before opening.

Subfile names must consist of alpha (i.e., A-Z) or numeric (i.e., 0-9) characters, a blank and/or a dash (-) only. The blank and the dash must not be used as the first character of the subfile name. An example of the correct use of these characters is 245B-BA-1234567-SUS. Special characters and symbols must not be used as subfile names in administrative or investigative case files.

The use of special characters and symbols (e.g., &, ^, %, #, etc.) as subfile names in electronic recordkeeping systems may cause unexpected errors especially when uploading or migrating data between electronic systems. As a result, data fields may not populate correctly and data may be lost. The use of special characters and symbols as subfile names may also impede the user's ability to upload data or perform searches in electronic recordkeeping systems.

Appendix J of the Domestic Investigations and Operations Guide 0667DPG contains a list of standardized subfile names which must be used when creating subfiles to document specifically described investigative or administrative activity [redacted] b7E

[redacted]

b7E

With the advent of Sentinel and electronic recordkeeping, it is not necessary to create a separate subfile for classified information. Since Sentinel is classified up to the Secret classification level, it is acceptable for Secret, Confidential, and Unclassified serials to be contained in the same case. Each serial should be classified at the highest level of classification for the content of that serial (i.e., if the case title is classified, and that title appears in the document, the entire document/serial is classified). In addition, if the case content, containing both classified and unclassified serials, is printed into paper format or copied to electronic data storage media, then all of the material needs to be protected at the highest level of classification contained in the material. See Section 5.11 below for additional guidance.

If a paper subfile is created for Secret classified material, only the paper subfile is classified Secret. The main file and all other subfiles are not classified Secret provided they do not contain any classified material.

Sentinel Online Help contains instructions for creating subfiles in Sentinel.

5.6.1. Grand Jury Subfiles

A grand jury subfile may be used to segregate, safeguard, and store federal grand jury material. Although Sentinel, from an information technology standpoint, can restrict access to documents, there are many occasions when it is necessary to illustrate to the court and others the FBI has maintained the integrity of grand jury material and has housed it in specific uniform locations. The Domestic Investigations and Operations Guide 0667DPG sets forth Bureau policy concerning treatment of federal grand jury material.

5.7. 1A (FD-340) Envelopes

This guidance is limited to non-evidentiary items; FBI personnel should continue to follow the Field Evidence Management Policy Guide 0780PG for guidance about the storage of evidence.

The 1A (FD-340) is a small clasped envelope which holds documents or items of non-evidentiary, non-chain-of-custody property pertinent to an investigation. Historically, there have been several different envelope sizes used (e.g., FD-340, FD-340a, FD-340b, and FD-340c).

Before the advent of Sentinel, 1A envelopes were typically received stapled or paper-clipped to a document (e.g., an EC or FD-302). The document was uploaded and serialized, and the file number and serial number were placed in the lower right corner of the document. The serial number of the document was placed on the 1A envelope "serial number of originating document" line. The 1A was entered into Collected Items, which generated a 1A number. The number was placed on both the 1A and on the document. Both documents were then filed in the case file.

As a cost saving initiative, and after canvassing all records liaisons for their views and having received their feedback, the FBI has determined it will no longer use the following types of 1A envelopes for non-evidentiary material: FD-340, FD-340a, and FD-340b. Offices may continue to use the FD-340, FD-340a, and FD-340b until current supplies are depleted. Going forward, the only 1A envelope available for use will be the FD-340c. In instances where hard copies of an item must be maintained, an accordion folder will hold the FD-340c for the collected items.

Sentinel Online Help contains additional information about 1A attachments in Sentinel.

5.8. Compressed Files

The use of compressed files is no longer authorized. Each paper file must be maintained as an independent volume. Electronic recordkeeping systems, such as Sentinel, will create a separate electronic file for each new case.

Compressed files were small paper case files (normally one to ten serials in scope) opened in the same file classification and placed together in a single file jacket in order to conserve shelving space. The process of compressing files created a burden when the records were eligible for disposition review. Not all the case files contained within the same compressed volume shared the same disposition. One or more of the case files may have met the criteria for permanent retention and transfer to NARA, while other files within the same volume may have been eligible for destruction. As a result, the disposition reviewer had to spend additional time manually separating the case files. An additional issue arose when file jackets listed case files not actually maintained within the compressed volume. For example, a compressed file might be marked as containing case files 91-123 through 91-129; however, the actual case files maintained within the compressed volume were 91-123, 91-124, 91-125, and 91-129. Case files 91-126 through 91-128 were maintained as separate files but the file jacket was not marked to reflect this. Therefore, when the disposition reviewer received the compressed file and analyzed it for retention / destruction, it appeared case files 91-126 through 91-128 were missing from the file jacket.

5.9. File Consolidation

Case consolidation is the process of moving one case's contents into another case. The requesting office must close a case in order for it to be consolidated into another case. The new case should already be opened in Sentinel, and pending evidence must have been transferred to the new case file. Keep in mind that 1As are consolidated only when attached to a serial.

To consolidate a case in Sentinel, set a lead to [redacted] For case consolidations, set the lead from the receiving case, the case into which the closed case is being consolidated. b7E

Before Sentinel, paper files were consolidated when there were two or more files on the same subject pertaining to related or similar matters. Files were consolidated by:

1. Writing "Consolidated into _____ (new file number)" on the front of the eliminated file

2. Retaining the empty file jacket cover in the closed files section

Files were also consolidated when the OO was re-designated.

5.10. Dual Captioned Cases

Dual captioned cases are not used in Sentinel.

Before Sentinel, when an investigation crossed over dual programs, a dual captioned investigation was opened. A dual captioned investigation was prepared as any other investigation with the exception of a dual caption or title. An example is as follows:

HENRY WILLIAM JONES

COMPUTER INTRUSION and STOCK MANIPULATION

288A-DL-123456

318C-DL-123457

The above example may have been handled by a cyber squad in one of the Dallas resident agencies and by a white collar crime squad located at Dallas headquarters.

5.11. Cover Sheets and Media Labels

Cover sheets, Sensitive Compartmented Information (SCI) sheets, and media labels protect information and material by providing visual protection from casual observation. Cover sheets conveying the highest classification of information in the document, (e.g., top secret (SF-703), secret (SF-704) and confidential (SF-705)), must be attached to the front of classified documents to safeguard the information when it is removed from protected storage. SCI cover sheets (SF-704-101) must be used to cover sensitive compartmented information. Media labels must be conspicuously placed on all media according to the highest classification level of the information ever stored or processed on the media. Unclassified media must also have a color-coded label and data descriptor label. Data descriptor labels are used to provide information about additional controls placed on media. The label should indicate, at a minimum, classification level, dissemination, access, handling, and other controls. The data descriptor label used is the SF-711, or its equivalent. See External Security Marking of Information Technology Hardware and Electronic Data Storage Media Corporate Policy Directive 0636D for additional information.

5.12. Controlling Top Secret/Sensitive Compartmented Information (TS/SCI)

The Security Division, Information Security Team's National Security Information Program manages policy, training, oversight, and coordination of Headquarters-level efforts and programs in regard to classifying, declassifying, and safeguarding national security information in accordance with EO 13526, ISOO Directive No. 1, and the

Intelligence Community marking format. Information regarding classification management can be found on the Security Division's National Security Information Program's webpage.

5.12.1. **TS/SCI Documents – Sentinel**

The Sentinel application is classified at the Secret level. The text of all documents classified at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, to include [redacted] material classified at the TS/SCI level, is prohibited from being uploaded into Sentinel.

The existence of a TS/SCI non-transitory record [redacted] however, must be documented in Sentinel utilizing a "placeholder." Use the FD-1057 (EC) and 1A/1C package function in Sentinel to create a "placeholder" for the document.

To properly record the non-digital TS/SCI document:

1. Portion mark the EC as Unclassified.
2. Type [redacted] b7E
3. Add a 1A/1C package to the EC.
4. Portion mark all metadata as Unclassified.
5. Select 1A as the package type.
6. Enter the phrase [redacted]
7. Click [redacted]
8. Portion mark all fields as Unclassified.
9. Enter the phrase [redacted]
10. Select [redacted] as the attachment type.
11. Click [redacted] to attach the 1A package.
12. Select the [redacted]
13. Select the [redacted]
14. After final approval of the EC, access Sentinel to print a copy of the EC. Click the "Print" icon in the serial viewer. The printed copy will contain the file and

serial number. [redacted] b7E
PDF will not have the serial number.

15. Attach the TS/SCI documents to the printed EC, and place the documents into a 1A envelope.

16. The TS/SCI material must be maintained in a Sensitive Compartmented Information Facility (SCIF) in accordance with TS/SCI storage and maintenance policies.

5.13. Case Status

5.13.1. Closing a Case – Sentinel

Sentinel Online Help sets forth instructions for closing cases in Sentinel.

5.13.2. Closing a Case – Paper Record

When a case is closed, on the file jacket cover, mark a line through the assigned Special Agent / squad name and on the line above write a "C" and the date the file was closed in the case management system. The following notations should be used:

- C4 – Administrative Closing
- C5 – United States Attorney (USA) Declination
- C6 – Other

5.13.3. Pending Inactive

A case is in pending inactive status when investigative activity is completed and only prosecutorial action or other disposition remains to be determined and reported.

With paper records, when the status or assignment of a case is changed, the top of the file jacket cover is marked accordingly. Mark a line through the assigned SA / squad name and on the line above write a "P*" and the date to indicate it is pending inactive. In fugitive cases, refer to Section 4.10, "Pending Inactive Status when all Logical Investigation has been Conducted," in the Fugitive Policy Guide 0404PG.

5.14. Records Managed by the Executive Secretariat

Correspondence addressed to the FBI from Congressional, Department of Justice (DOJ), White House, and other government sources is received, disseminated for response, and reviewed by the Executive Secretariat (Exec Sec). Executive level correspondence includes correspondence written to or signed by the Director.

Executive correspondence received from external sources as well as memoranda, correspondence, letters, and other documents received, signed, and reviewed by the

Director and other FBI executives are maintained in an electronic recordkeeping system known as Correspondence and Electronic Request Management (CERM) which has been approved by NARA as an official recordkeeping system and is managed by Exec Sec. Paper copies, if created, may be maintained for three months for convenience only.

6. Administrative Files - Classifications 319 / 67Q

The FBI creates administrative records to facilitate day-to-day organizational and housekeeping activities. Routinely created administrative records include travel vouchers, purchase orders, and budget preparation documents.

The Archivist of the United States issued the General Records Schedules (GRS) to provide disposal authorization for temporary administrative records common to several or all agencies of the federal government. The RMD has adapted the GRS for FBI use and has designated Classifications 319 and 67Q as the filing locations for administrative records.

Records subject to a legal hold, special inquiry, or Freedom of Information and Privacy Acts (FOIPA) requests are not to be destroyed even if their retention period has been met under the GRS. This is true for all records – investigative and administrative. In these circumstances, the OGC should be contacted for instruction.

6.1. Classification 319 – Administrative Matters

Each of the GRS chapters has been assigned a 319 alpha character. Each alpha has been further broken down into a records series with each series corresponding to a separate body of records. Each series has been assigned a main file number, which has been further broken down into subfiles corresponding to each division, field office, or LEGAT designator.

Only documents of FBI-wide interest or significance are filed in the main file. Subfiles are used for those records not disseminated widely (i.e., FBI-wide or to all field offices) and do not have significance beyond the individual office.

Individual sections and units are not authorized to create further subfiles for their administrative records. For example, all budget correspondence created by the RMD will be filed in the subfile for the RMD's budget matters (319D-HQ-A1487519-RMD) regardless of whether the Records Policy and Administration Section (RPAS) or the Records Automation Section (RAS) created the record. See the Classification 319 Guide for detailed information about each 319 alpha file classification.

Not all offices will have a need to use every established case file number and it is not necessary to import into each file. For example, Jacksonville may create records related to Space Matters (319J-HQ-A1487567-JK), while the OGC may never have a need to file any records in their Space Matters subfile.

Particular attention should be given to 319T-HQ-A1487667, Office Administration. This file should be used to house records related to the internal administration of an office. Records filed here relate to staffing matters (night, weekend, and holiday duty), internal office procedures, and other housekeeping records. Only the subfiles for this file are to be used, as records filed here relate to matters not having significance beyond the creating office or squad.

6.2. Classification 67Q – Administrative Personnel Records

Classification 67Q covers the disposition of administrative records related to personnel matters. These records relate to the supervision, administration, and management of FBI personnel. Included in this classification are categories for hiring, career boards, performance appraisals, benefits, and similar personnel issues.

GRS Chapter 1 covers administrative personnel matters. The disposition authorities contained in GRS Chapter 1 have been linked to the 67Q file categories. A main file and subfiles for each division, field office, and LEGAT, have been created for each of the 67Q categories. Again, not all offices will have a need to use every established case file number. Additionally, it is not necessary to upload into each file. For example, there is no need to upload supervisor's drop files. Supervisors should establish a paper file named 67Q44 (Supervisor's Drop File) in which to store these records. These files can then be managed according to the appropriate disposition instructions. See the Classification 67Q Guide for detailed information and disposition instructions.

6.3. Filing Exceptions to Classifications 319 / 67Q

Certain categories of administrative records should not be filed in Classifications 319 or 67Q:

- Records related to the investigation of automobile accidents should be filed in Classification 66A; all other records related to the maintenance and operations of motor vehicles should be filed in the appropriate file number within 319I
- Training records should be filed in Classification 1
- Administrative records related to the President's Intelligence Oversight Board (PIOB) should be filed in Classification 278
- Records related to forfeitures should be filed in the related investigative case file; however, copies of administrative and financial records related to the Asset Forfeiture and Abandonment Programs, including lists and reports of seized assets submitted to HQ for processing, may be filed in 319C-HQ-A1487518 (Forfeiture Matters)
- Records related to specific FBI information systems (such as NCIC or Guardian) should be filed in corresponding Classification 242 case; however, records

relating to general automation matters (such as Automation Requests) should be filed in a Classification 319U category.

6.4. Management of Classification 319 / 67Q Files

Good records management practices dictate administrative files (i.e., Classification 319 and 67Q) be segregated from investigative or intelligence files. Classification 319 and 67Q files should be placed in a file drawer or cabinet separate from these files.

Each Classification 319 file container (file front / back, drop folder, accordion folder) is identified by the:

- Classification number and alpha character
- Case file number
- Title of the 319 category as it appears in the Classification 319 Guide
- Calendar or fiscal year in which the files were created or received.

If additional volumes or sections are created during the year, they must be identified by a new, sequential volume or section number and the timeframe they cover (e.g., April - May 2013). At the end of the calendar or fiscal year, the series must be closed, or "cut off," and a new series begun for the new calendar year. The new series should begin with a new volume or section (i.e., volume 1) and continue sequentially through the year as needed.

The 319 file numbers may be displayed on both serialized and unserialized documents in case files. Note: It is necessary to display the file number on records in 319 categories which are not uploaded to Sentinel. The main file number is displayed on documents as 319I-HQ-A1234567 and the subfile number is displayed on documents as 319I-HQ-A1234567-AL.

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

Office Administration
Records Management Division
Policy, Analysis, and Compliance Unit
Emergency Wardens Contact List

6.5. Filing Responses to 319/67Q Files in Sentinel

A response to a document is always filed in a subfile, not the main file. Two examples follow. First, if the Finance Division (FD) sends out a Bureau-wide EC, it is sent from the HQ main file. All responses to the EC are to be filed in the subfile of the responding office. For example, when the Baltimore field office (BA FO) responds, the response will be filed in the BA FO subfile, not the HQ main file. The BA FO response should

reference the HQ file and serial number to which it is responding. Second, if the FD is communicating solely with the BA FO, then the FD should file its communication in the FD subfile. If the BA FO responds to the communication, then the BA FO should file its response in the BA FO subfile and reference the FD's file and serial number.

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

6.5.1. Serializing 319/67Q Files in Sentinel

Not all administrative documents are serialized into Sentinel. For example, time cards are not serialized.

Documents serialized into Sentinel are identified by the appropriate 319 case file number. An example of a main file number is 319W-HQ-A1487697 and a subfile is 319W-HQ-A1487697-RMD. The title of the document will automatically populate in Sentinel. Originators serialize to either the main or a subfile, whichever is appropriate, but not to both.

Divisions must designate those administrative files requiring supervisory approval prior to importing and serializing in Sentinel. Unless specifically designated, supervisory approval is not required for importing and serializing administrative records. When supervisory approval is required, divisions and offices must establish clearly defined procedures for obtaining required signatures which will not impede the timely serialization of records in the administrative case file.

6.6. Administrative Records Checklist

Below is a checklist to help each office properly organize and manage its administrative files:

Managing 319 and 67Q Files		
1.	Is a system of records set up for Classification 319 and 67Q categories used by the office?	☐ Yes ☐ No
2.	If paper records are being maintained, is the file drawer/cabinet or other storage area clearly identified with Classification 319 or 67Q and the calendar/fiscal year? Note: The RMD recommends creating electronic records and developing a file plan to maintain them on a shared drive, as stated in Section 3.	☐ Yes ☐ No
3.	Is each file folder identified with: — the correct Classification 319 alpha or 67Q case number — the corresponding title — the date span of the records	☐ Yes ☐ No
4.	Are additional volumes or sections opened during the calendar/fiscal year correctly identified?	☐ Yes ☐ No
5.	Is the file appropriately designated as a subfile?	☐ Yes ☐ No
6.	Are closed or cut-off files regularly set apart from active files?	☐ Yes ☐ No
7.	Are new volumes or sections opened at the beginning of each calendar / fiscal year?	☐ Yes ☐ No
8.	Are documents identified with the appropriate 319 alpha or 67Q case file number?	☐ Yes ☐ No
9.	If required, are original paper copies of documents, imported to another division's subfile, sent to the division to be filed?	☐ Yes ☐ No
10.	Are non-record duplicates or working copies separated from the official files and regularly purged?	☐ Yes ☐ No
11.	Does the office create documents in Sentinel when appropriate?	☐ Yes ☐ No
12.	Are imported documents identified with the correct 319 case file number(s)?	☐ Yes ☐ No

Managing 319 and 67Q Files		
13.	Do imported documents have the title in the correct format (corresponding to the document's case file number)?	☐ Yes ☐ No
14.	Are responses to 319 correspondences filed in the originator's main or subfile?	☐ Yes ☐ No
15.	Are documents filed in both the main and subfile?	☐ Yes ☐ No

7. Personnel Files

7.1. Official Personnel Folder

The official personnel folder (OPF) is a group of records documenting an FBI employment history with the federal government. As of March 2013, OPFs have been converted to electronic official personnel folders (eOPF).

In addition to the OPF, the FBI maintains a file classification 67 case file on each applicant and employee. The employee files may also include a security subfile (sub-S), medical subfile (sub-M), or financial subfile (sub-F). The official record is comprised of records maintained electronically within Sentinel and in some instances in paper format.

The official paper version of all FBI personnel records excluding the e-OPF, regardless of the FBI employee's office assignment, is maintained at the Alexandria Records Center (ARC).

7.2. Requesting a Copy of FBI Personnel Records

Current personnel may print and save copies of their e-OPF at any time during their employment. Current employees may also request copies of their medical information from the FBI Health Care Programs Unit and/or other FBI medical personnel. For other materials in one's personnel file, or for requests by former employees, current and former FBI personnel may request a copy of their FBI personnel records by submitting a Privacy Act Request to RMD. This can be done in two ways.

First, complete and sign a copy of the U.S. Department of Justice Certification of Identity Form DOJ-361 (Form DOJ-361). This form is also available at www.fbi.gov/foia/requesting-fbi-records.

Alternatively, following the instructions contained in Form DOJ-361, submit a letter to the FBI, sign and have it notarized or state the following: "Under penalty of perjury, I

hereby declare that I am the person named above and I understand that any falsification of this statement is punishable under the provisions of Title 18, United States Code (U.S.C.), Section 1001 by a fine of not more than $10,000 or by imprisonment of not more than five years, or both; and that requesting or obtaining any record(s) under false pretenses is punishable under the provisions of Title 5, U.S.C., Section 552a(i)(3) as a misdemeanor and by a fine of not more than $5,000."

Mail, fax, or e-mail the completed Form DOJ-361 or letter to:

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

Fax: 540-868-4391 / 4997

E-mail (scanned copy): foiparequest@ic.fbi.gov

8. Storing Records

FBI records are stored in FBIHQ divisions, field offices, LEGATs, off-sites, and in electronic systems.

The Security Division's Closed/Open Storage Secure Area Approval Program sets forth the physical security features necessary to protect classified information up to the Secret collateral level at resident agencies and off-sites and the closed storage of Top Secret information at FBIHQ and field offices. Closed/Open Storage Secure Area Checklists are posted on the SecD's website.

8.1. Storing Files at the ARC

Most FBIHQ closed-case files are stored at the ARC, which is managed by the RMD's Records Storage and Maintenance Unit (RSMU). FBIHQ divisions send records to the ARC for storage. Records remain in the OO until they become less active.

FBIHQ records with a classification higher than Secret or containing Sensitive Compartmented Information (SCI) are stored in the Special File Room at FBIHQ, Room [redacted] Similar records in field offices are stored in secure areas. b7E

Administrative records covered by Classification 319 which relate only to individual unit activities are not stored at the ARC. Instead, these administrative records should be stored at the unit level; their location should be reflected on the unit's file plan.

8.2. Storing Files at a Field Office or Resident Agency (RA)

All files are maintained in the headquarters city unless the RA location is in compliance with the requirements for classified material storage as set forth by the Security Division. To maintain pending original / duplicate files in an RA location, the office must have received approval for open storage of classified material by the Security Programs Manager (SPM), Security Division (SecD), FBIHQ.

Top Secret or SCI documents / materials may not be maintained in the RA unless a demonstrable operational need is shown, prior approval is granted by the SPM at FBIHQ, and the storage facility is in compliance with the requirements for the storage of such material. Confidential human source files are maintained in the headquarters city, as is all information which identifies an informant or asset.

Foreign counterintelligence (FCI), sensitive organized crime, public corruption, and undercover operation files are maintained in the headquarters city, unless the Special Agent in Charge (SAC) or Assistant Special Agent in Charge (ASAC) has personally determined on a case-by-case basis that retention of the file in the RA is necessary to effectively conduct the investigation, and the files are retained in a secure manner. SACs / ASACs cannot delegate this authority. Justification and authorization to retain the files are documented by memorandum to the case file(s).

All files must be returned to the headquarters city within 30 calendar days of the date the file was closed. Prior to closing the file, a serial by serial match with the original paper file, if one exists, and the central recordkeeping system (Sentinel) is conducted to ensure all serials are appropriately filed. All original serials and exhibits are included in the file at the time it is sent. However, documents imported or created in Sentinel do not have to be printed and added to a paper file.

The transport of files in bulk between the headquarters city and the RA, and vice versa, must be done in accordance with Security Division requirements.

8.3. Storage Facility Standards

The law governing facility standards for records storage is set forth at 36 C.F.R. Part 1234. It applies to all records storage facilities that federal agencies use to store, service, and dispose of records. It specifies the minimum structural, environmental, property, and life-safety standards a records storage facility must meet to store federal records.

All records, regardless of medium, must be stored to meet environmental standards and preservation requirements. All records should be removed from desk tops at the end of the business day and placed in proper storage containers. All records should be properly protected in appropriate storage to deter damage from negligence, accidents, disasters, or emergencies.

Table 1 sets forth the recommended temperature and humidity levels for records storage.

Media	Temperature	Relative Humidity (RH)	Reference
Paper-based temporary records	Should not exceed 70º Fahrenheit. Ideal between 40º and 68º Fahrenheit	30-50% RH; do not exceed 50%	36 CFR §1234.14 (a)
Paper-based permanent and unscheduled records	Between 40º and 65º Fahrenheit	20-50%RH; do not exceed 50%	36 CFR §1234.14(c)
Optical – CDs/DVDs	Between 39º and 68º Fahrenheit	20-50% RH	National Institute of Standards and Technology

Microfilm/Microfiche	Should not exceed 68º Fahrenheit	35% RH (+/- 5%)	36 CFR §1238.20(a), American National Standards Institute IT9.11-1993

8.4. Common Storage Containers

The common storage containers chart contains a list of pros and cons for the various containers explained in detail below.

8.4.1. Vaults/Fire-resistant Safes

Vaults and fire-resistant safes offer the highest form of protection to FBI records. They are also the most expensive. Offices should consider housing vital records in these types of containers as these records are the most important to the continuity of the FBI.

8.4.2. Filing Cabinets

Filing cabinets are the ideal protection for FBI records as they are secure and the metal will not absorb or retain water. Ensure the cabinets meet the minimum six inch requirement off the floor; otherwise do not utilize the lower cabinet for FBI records.

8.4.3. Open Shelving

FBI records are often stored on open shelving as it provides more storage space than filing cabinets and is also less expensive. Should your office determine open shelving will house FBI records, ensure there is plastic sheeting available to cover and protect records from water and wind damage when needed. Additionally, ensure the plastic sheeting can be secured in the event of high-wind situations.

8.4.4. Plastic Containers

Plastic containers protect FBI records from water more effectively than a cardboard box. However, records stored in such a container are vulnerable to increased temperatures when the container is closed. Temperatures inside the container will continue to increase when containers are stacked. If used, ensure plastic containers are located in a room with a lowered temperature so records contained within the containers comply with the temperature and humidity levels set forth in 36 CFR Part 1234 and 36 CFR Part 1238.

8.4.5. Cardboard Boxes

If cardboard boxes are utilized for records storage, records should be stored in one cubic foot Federal Records Center boxes. These are standard U.S. General Services Administration (GSA) boxes and can be obtained through a (GSA) catalog or GSAadvantage.com. The item number is 8115-00-117-8249. These are the same

boxes required for shipping files to the ARC. Banker's boxes and Xerox boxes are not acceptable protection or storage for FBI records.

8.5. Storage for Electronic and Audiovisual Records

Electronic and audiovisual records must be imported into Sentinel, the FBI's central recordkeeping system. If electronic and audiovisual records are also kept in original, analog format, they should be stored in accordance with the following instructions:

- Store magnetic media, including open-reel sound recordings and video cassettes away from other electronic devices, in containers made of polypropylene, polyethylene, or non-corrosive material
- Store tapes, CDs, and DVDs vertically in jewel cases or plastic containers to protect them from dust and debris
- Store in secure areas protected against unauthorized access and from exposure to 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
- Prohibit eating, drinking, and smoking in facilities except in designated areas. If eating or drinking at a workstation, maintain an appropriate distance from records as a spill could damage or destroy records, equipment, or information

8.6. Strategies for Storage in Anticipation of Natural Disaster

In the event of a natural disaster, ensure all records are elevated more than six inches off the floor. Remove all records from desk tops and secure in filing cabinets. Lock all cabinetry to protect them from opening if picked up by high-winds. Duplicate and disperse vital records. Anchor any equipment to solid walls and beams in the event of an earthquake, but keep away from plumbing or pipes. If possible, relocate all records to a centralized location in the middle of the building, floor, or to room(s) without windows. If this is not possible, cover everything with plastic sheeting and move as far away from windows as possible.

9. Transferring Records within the FBI

9.1. Transferring Records in Sentinel

Case ownership may be transferred within a field office or to another field office. If one or more field offices are assisting the originating field office with a case, the case manager can share ownership by assigning a case manager from the assisting field office(s) to the case. Sentinel Online Help contains instructions for change case requests.

If a case is being transferred from one field office to another field office; the originating field office must close the existing case, the field office taking over the case must open a new case, and then the two cases must be consolidated. The RMD One Shot Library contains an instructional aid for requesting case consolidations. For additional assistance, contact the RMD Help Desk at [redacted] or by e-mail at [redacted] b7E

9.2. Transferring Records to the ARC from FBIHQ and Field Offices

To transfer records to the ARC for storage, the transferring office must submit a lead request to [redacted] at least two weeks ahead of the intended shipping date. The lead should indicate the volume, classification, date span, servicing requirements, and disposition, if known, of the records. The lead request must also include the type of medium contained in the file, if any, in addition to paper (i.e. CD, DVD, etc.). When RSMU receives the lead request, the Unit Chief or designee will review and make a determination as to whether the records are appropriate for storage at the ARC. b7E

If RSMU approves the storage, ship the records to the ARC in the following manner:

1. Arrange and ship records in white, standard General Services Administration (GSA) boxes. These boxes are available through the GSA; the GSA box number is NSN 8115-00-117-8249 and the measurement is 14 ¾ X 12 X 9 ½. Other boxes, including banker's or Xerox boxes, cannot be accepted because they do not provide adequate protection for the records.

2. Organize pre-UCFN records by file classification and then by case number, in sequential order.

3. Organize UCFN records by case number, in sequential order.

4. Bulkies and Enclosures Behind File (EBFs) are large items which do not fit in the file but are a part of the file. These items include, but are not limited to, cardboard tubes, presentation boards and large collections of material. Include bulkies and EBFs in the box with the corresponding case file. Do not place bulkies and EBFs in separate boxes unless volume warrants it.

5. Mark identification information in black marker on each box. Write the information on the side of the box which contains the statement "**Do not write on this side**." DO NOT write any information on any other side of the box as those sides of the box are used when transferring records to NARA. Each box must indicate the individual box number and the entire box count, (e.g., box 1 of 10).

6. List the entire case number including classification on the outside of the box. If more than one case is in a single box, all case numbers must be indicated. If the number of cases in a single box is voluminous, include a complete list of cases inside the box instead of writing them all on the outside of the box.

7. If more than one box is used for a case, the case number is 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 the boxes.

8. 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.

9. Create a list of the records being shipped, including the name of the office, unit, section, and division shipping the records; the name and telephone number of a point-of-contact; and a detailed and complete listing of the contents of each box. Create three copies of the list: place one in the first box of the shipment, send one to the ARC, and maintain one in the office as a reference. Also, send an electronic version of the inventory to the Unit Chief, RSMU, RMD via a lead in Sentinel.

10. Please note, all case documents must be serialized prior to transfer to the ARC. Any case documents received at the ARC without a file and serial number will be returned to the submitting office.

For additional information, see electronic communication (EC), dated 6/19/2002, entitled "Security Requirements for Shipping / Receiving FBI Documents and Related Material Within the United States and Puerto Rico," 261D-HQ-C1188941serial 894.

9.3. Transferring Records to the ARC from LEGATs

To transfer records to the ARC for storage, the transferring office must submit a lead request to [redacted] at least two weeks ahead of the intended shipping date. The lead should indicate the volume, classification, date span, servicing requirements, and disposition, if known, of the records. The lead must also include the type of medium contained in the file, if any, in addition to paper (i.e., CD, DVD, etc.). b7E

When RSMU receives the lead request, the Unit Chief or designee will review and make a determination as to whether the records are appropriate for storage at the ARC.

If RSMU approves the storage, ship LEGAT office files to the ARC in the following manner:

1. Arrange and ship records in white, standard General Services Administration (GSA) boxes. These boxes are available through the GSA catalog ordering process. The GSA box number is NSN 8115-00-117-8249 and the measurement is 14 ¾ X 12 X 9 ½. Other boxes, including banker's or Xerox boxes, cannot be accepted because they do not provide adequate protection for the records.

2. All records in each box should have the same classification unless the box has additional space

3. Include bulkies in the box with the corresponding case file. Do not place bulkies in separate boxes unless volume warrants it.

4. Wrap the outside of the box (es) with plain brown paper. Put the number of the box, (i.e., 1 of 1, 1 of 2, 1 of 3), on the brown paper on the outside of the box. Each box must indicate the individual box number as well as the entire box count.

5. Create a list of the records being shipped, including the name of the office, unit, section, and division shipping the records; the name and telephone number of a point-of-contact; and a detailed and complete listing of the contents of each box. Create three copies of the list: place one in the first box of the shipment, send one to the ARC, and maintain one in the office as a reference. Also, send an electronic version of the inventory to the Unit Chief, RSMU, RMD via a lead in Sentinel.

6. Please note, all case documents must be serialized prior to transfer to the ARC. Any case documents received at the ARC without a file and serial number will be returned to the submitting office.

In all cases, ship the boxes to the following address: Federal Bureau of Investigation,

[redacted] b7E

10. Retrieving Records

Authorized FBI personnel may request files in storage.

10.1. File Automated Control System (FACS)

The File Automated Control System (FACS) was a library system used to track the check out and return of all FBI Headquarters files (investigative, administrative, and personnel).

In June 2014, FACS was discontinued as a file request system and its data was exported to TRIM for interface with FRAP (File Request Automation Project). All file requests must now be submitted via FRAP.

10.2. File Request Automation Project (FRAP)

FRAP is an electronic system used for requesting all FBI files, including: (1) closed FO files sent to the ARC for storage as part of the RMD's Field Office Inventory Project and (2) LEGAT files stored at the ARC. The system has been constructed using SharePoint and InfoPath and is deployed on FBINet.

Before requesting a file, check TRIM to determine the file's location. If the file is at a FO, contact the FO to request the file. If the file is located at the ARC, access the FRAP website and follow the instructions for ordering a file. Once the request is received, RSMU will check the file out and either physically or electronically send it to the requester. When physically sent, a copy of the FRAP request form will be attached to the file for easy identification. The FRAP request form should be kept attached to the file.

The FRAP User Guide contains step-by-step guidance and additional information about this system.

10.3. Returning Files to the ARC

All paper files must be returned to RSMU within 90 days of receipt unless the requester requires additional time. To retain a file longer than 90 days, the requester must inform RSMU personnel through the FRAP.

If a file was provided in an electronic format (e.g., as a PDF or through a hyperlink), the electronic copy is a working copy and must be destroyed when no longer needed.

When returning a file ordered through FRAP, ensure the FRAP request form is attached to it.

10.4. Retrieving Personnel Records from the National Personnel Records Center (NPRC)

To obtain a file transferred to the NPRC, please complete an SF-127 form and submit it to the Records Policy and Administration Section Chief or Assistant Section Chief for approval. Upon approval, fax the completed SF-127 form to [redacted] Use of the SF-127 is restricted to authorized representatives of federal personnel offices. Please submit a separate request for each file requested. Specify on the SF-127: b7E

- Current and former name of FBI personnel
- Name of the agency (or agencies) of employment
- Dates of employment for which the records are desired
- Social Security Number for a United States citizen
- For foreign nationals, enter FNO in place of Social Security Number
- Date of birth
- Requesting agency's name and contact number

If the form is incomplete, it will be returned. Please return the file when no longer needed to:

National Personnel Records Center Annex
1411 Boulder Boulevard
Valmeyer, IL 62295

11. Imaged (Converted) Records

Divisions considering the conversion of records created in one particular media/format to another media/format must have authorization from RMD's Records Management Application Unit (RMAU). The RMAU will provide guidance on the process.

All hardcopy textual and non-textual documents scanned and converted to digital images must comply with the minimum requirements specified in Records Management Standards for Scanned Documents Policy Directive 0774D.

Some factors which may lead to a change in media:

- There is a legal requirement (e.g., 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 non-standard and/or no longer supported by the manufacturer
- Another format would better meet business needs
- The current format or media is not supported by FBI recordkeeping systems

Images may also be converted to searchable files through the use of Optical Character Recognition (OCR) software resulting in full text searchable files.

The decision to convert records to images or OCR them is 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 short retention periods
- Legal consequences if records are not retained in their original paper format (i.e., paper copies may be needed for original signatures, other authentication measures, or forensic analysis)

11.1. Recordkeeping Requirements for Imaged Records

Prior to conversion, RMD should evaluate records to determine if the originals can be destroyed once converted. Before files are destroyed, RMD examines the files to determine if disposition authority from NARA is required. In some cases, NARA and the FBI may agree to transfer the paper files rather than the scanned images. Therefore, when converting paper files to scanned images, offices must keep the paper files in a searchable arrangement until disposition authority is obtained. Offices desiring to maintain images should consult with RMD's RMAU for acceptable media, formats, and quality standards to be used so the storage of the images meets appropriate electronic recordkeeping requirements.

Evidence converted to digital format by RMD's DocLab is not 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., is returned to the contributor or destroyed in accordance with the Field Evidence Management Policy Guide 0780PG.

For large or priority scanning projects, contact the RMD's DocLab or send a request via e-mail to [redacted] b7E

12. Electronic mail (E-mail)

Sections 4.8.15 through 4.8.19 of the RM PG set forth policy regarding e-mail; they contain definitions for non-transitory record e-mails (needed for more than 180 days), transitory record e-mails (needed for 180 days or less), and non-record e-mails.

As set forth in the RM PG, FBI personnel must preserve non-transitory record e-mails in the appropriate electronic recordkeeping system. Copies of non-transitory record e-mails must be imported to the case file and indexed as appropriate before the original e-mail message in Outlook is deleted. Attachments, as well as transmission and receipt data about the e-mail, must also be saved as part of the record. Transmission and receipt data include the sender's name, date, subject, and recipient(s), and any requested return receipts.

12.1. Record Marking Tool (RMT)

The Record Marking Tool (RMT) is an automated marking tool in Microsoft Outlook used for designating e-mail as non-record, transitory record, or non-transitory record. Non-transitory record e-mails are forwarded to Sentinel for entry into a case file; this is necessary to ensure the information is available to others for investigative, analytical, and administrative purposes.

The use of the RMT is mandatory and applies to all e-mails on the Secret enclave (FBINet). As good stewards of FBI information, employees, contractors, task force officers, and detailees must understand and use the e-mail RMT when sending Bureau e-mails.

12.2. Manually Importing E-mails Received From Non-FBI Entities to Sentinel

FBI personnel may also receive e-mail from non-FBI entities (such as from a LEO e-mail account, fbi.gov account, ICE mail, SIPRNet, etc.) containing information pertinent to an investigation, to an intelligence gathering effort, to a significant administrative matter, or to other official FBI business. If these e-mails are non-transitory records, they must be imported into the electronic recordkeeping system. To prevent the introduction of viruses into the FBI systems, the following procedures should be followed when importing non-transitory record e-mails received from external Internet sources:

- Save the e-mail onto magnetic or optical media (e.g., FBI approved flashdrives, CD-ROMs, DVDs, etc.)
- Bring the media to your workstation and perform a virus scan to ensure neither the media nor the document contain viruses
- Follow the procedures outlined above to import the document to Sentinel

Alternately, FBI personnel may use "Uplift" on UNet to upload record e-mails or other documents containing record information to FBINet. The following procedures should be followed when using "Uplift" to upload non-transitory record emails:

From an FBI UNet computer,

- Save the e-mail as a [redacted] b7E
- Save any attachments.
- Virus scan all files you intend to send to the Secret enclave.
- Type in your browser address bar [redacted] and press Enter.
- Type in your [redacted]
- Select the files you want to send to the Secret enclave.
- Click "Upload Files".
- The documents will be sent directly to your [redacted] as an attachment.
- Save the attached documents to your network drive.
- Follow the standard importing procedures to import the document into Sentinel. NOTE: Do not upload the e-mail itself into Sentinel.
- Upload the e-mail's [redacted] file as the main document on the Import Form.
- Upload any attachments from the e-mail as digital 1As on the Import Form.

If the e-mail to be imported cannot be accessed on UNet, please consult your division's Chief Security Officer for assistance. For instructions on how to complete and submit the Import Form, please visit the Sentinel Resources site and view Quick Guide 7: FD-1036 Import Form.

For additional guidance and assistance, contact the RMD Help Desk at [redacted] or by e-mail at [redacted] b7E

13. Records Disposition

The elements of a records disposition program include development of retention schedules for all records, supervision of the storage of inactive records, management of the disposal of temporary records, and transfer of permanent records to NARA. The records disposition program applies to all records created in any medium.

Questions regarding records disposition may be e-mailed to RMD's Records Disposition Unit's (RDU) Help Desk at: [redacted] b7E

13.1. Records Scheduling

"Scheduling" is the process of developing mandatory instructions (also called disposition authorities) for handling federal records when they are no longer needed for agency business. The disposition of all federal records must be approved by the Archivist of the United States, who oversees NARA. The Archivist is the only individual in the federal government with the authority to approve the destruction, deletion, or removal of federal records.

FBI disposition authorities represent a legal agreement between the FBI and NARA. They set forth the requirements for disposing of records which have met retention requirements and provide instructions for identifying and transferring historically significant records to NARA. In addition to the disposition authorities for each file classification, disposition authorities have been, and continue to be, developed for the FBI's electronic information systems and other records falling outside the file classification system. For example, a disposition authority has been approved for the National Crime Information Center's electronic information system. The RDU is responsible for developing records disposition authorities for the FBI's paper-based records. The Records Management Application Unit (RMAU) develops disposition authorities for all electronic information systems.

The RMD assists FBI program managers with the review of new and existing records systems or paper series in order to evaluate and develop appropriate retention periods. In addition to working with program managers, the RMD also consults with the OGC, ITSD, the Office of Congressional Affairs, and other stakeholders who have an interest in the retention of the records. Following an internal review, the RDU prepares and submits to NARA a request for records disposition authority on a Standard Form 115 (SF-115). The RMD works with owners of paper records, IT system owners, and program managers to prepare disposition schedules.

NARA reviews the proposed disposition authority, works through the RMD to answer questions, prepares a written appraisal of the proposed request, and publishes a notice of the proposed disposition authority in the Federal Register. Following a public comment period and barring any concerns about the proposed retention period(s), the proposal is submitted to the Archivist of the United States for signature. Upon signature,

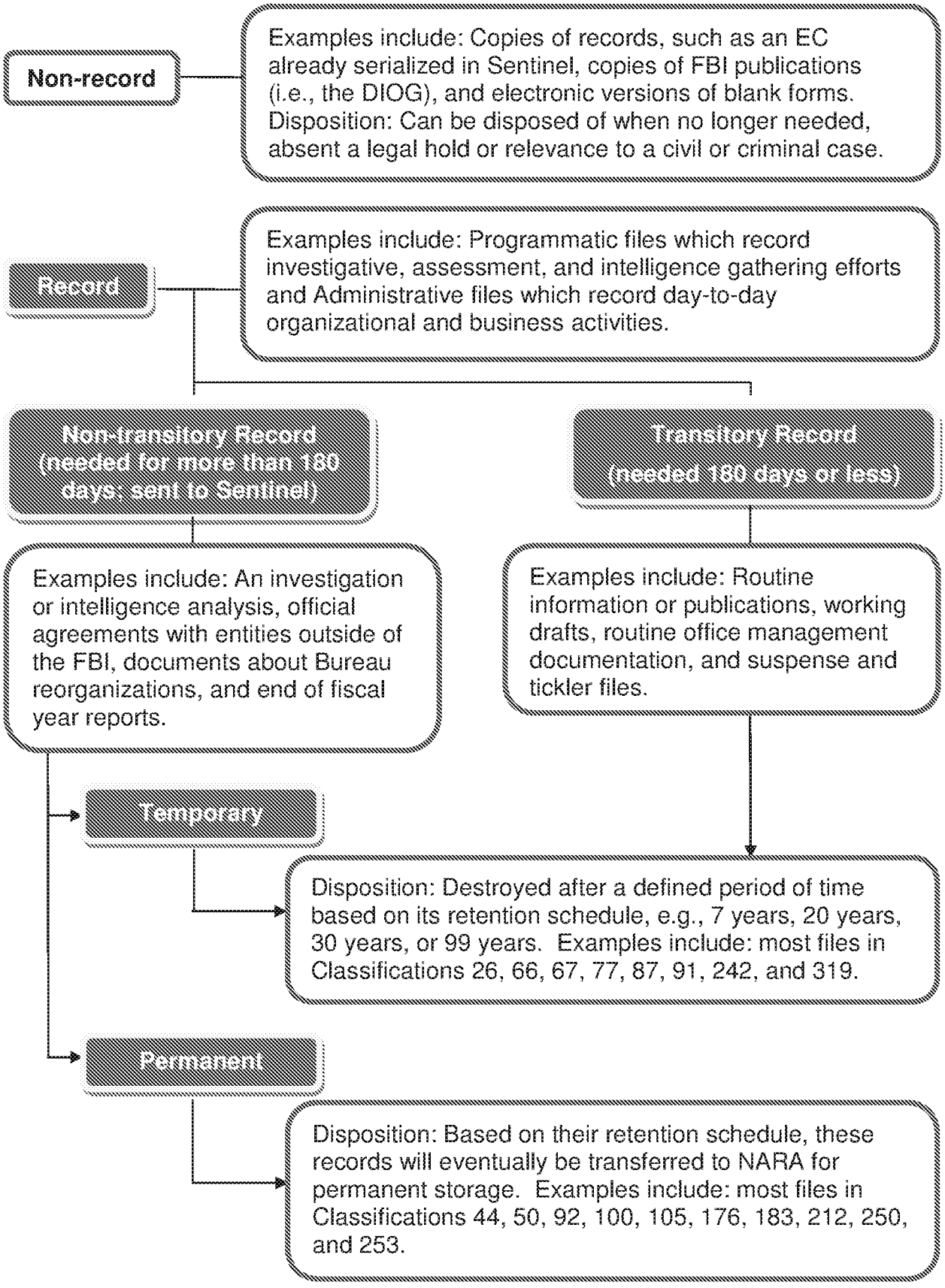
the disposition authority becomes a legal agreement between NARA and the FBI on the length of time the records will be retained.

13.2. **The FBI's Retention Plan**

Approved disposition authorities are compiled into a set of instructions for managing records. This compilation is called the FBI's 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 type), or for electronic information systems, 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.

Understanding what records are and their proper handling is the responsibility of the entire FBI workforce. It is important to be able to identify FBI records, but it is equally important to be able to distinguish between the different types of records. The flowchart on the following page contains examples of the different types of records and non-records you may encounter in your office's day-to-day operations.


Non-record
Examples include: Copies of records, such as an EC already serialized in Sentinel, copies of FBI publications (i.e., the DIOG), and electronic versions of blank forms. Disposition: Can be disposed of when no longer needed, absent a legal hold or relevance to a civil or criminal case.
Record
Examples include: Programmatic files which record investigative, assessment, and intelligence gathering efforts and Administrative files which record day-to-day organizational and business activities.
Non-transitory Record (needed for more than 180 days; sent to Sentinel)
Transitory Record (needed 180 days or less)
Examples include: An investigation or intelligence analysis, official agreements with entities outside of the FBI, documents about Bureau reorganizations, and end of fiscal year reports.
Examples include: Routine information or publications, working drafts, routine office management documentation, and suspense and tickler files.
Temporary
Disposition: Destroyed after a defined period of time based on its retention schedule, e.g., 7 years, 20 years, 30 years, or 99 years. Examples include: most files in Classifications 26, 66, 67, 77, 87, 91, 242, and 319.
Permanent
Disposition: Based on their retention schedule, these records will eventually be transferred to NARA for permanent storage. Examples include: most files in Classifications 44, 50, 92, 100, 105, 176, 183, 212, 250, and 253.

13.3. Non-Transitory Record – Temporary Retention

A non-transitory record with a temporary retention is a record deemed by NARA to have no continuing value after its usefulness to the FBI has ceased. These non-transitory 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, unless subject to a legal hold. Their retention period may range from months to years. NARA allows for the storage of temporary non-transitory records in any medium deemed necessary by the creating agency. For more information see 36 C.F.R. Part 1234, NARA Regulation General Records Schedule (GRS) 20, Item 3(a), NARA Regulation GRS 20 Item 3(b)(3), and NARA Regulation GRS 20 Item 3(b)(5).

13.4. Non-Transitory Record – Permanent Retention

A non-transitory record with a permanent retention is a record determined by NARA to be sufficiently valuable for historical or other purposes to warrant continued preservation by the federal government after its usefulness to the FBI has expired. Nearly every FBI file classification contains some permanent non-transitory records. For example, all domestic security records filed in Classification 100 are permanent and will be transferred to NARA after a specified time period.

13.5. Transitory Record – Needed for 180 Days or Less

A transitory record is a record which has only minimal documentary or evidentiary value and is needed for 180 days or less. Transitory records may include:

- Routine requests for information or publications and copies of replies requiring no administrative action, no policy decision, and no special compilation or research for reply.
- Originating office copies of letters of transmittal which do not add any information to the information contained in the transmitted material.
- Quasi-official notices and other records which do not serve as the basis for official actions such as notices of holidays, charitable events, etc.
- Records documenting routine activities containing no substantive information such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling-related activities.
- Routine communications such as reminders of existing policies, work-related guidance, and meeting notices.
- Drafts of or comments on proposed policies or actions not considered or submitted for consideration by the approving authorities.
- To-do lists.

13.6. Unscheduled Records

Records for which the disposition period has not been determined are called unscheduled records. These records have no authorized retention, destruction, or transfer instructions. Therefore, unscheduled records may not be destroyed. They are

kept until a retention schedule is approved for them, authorizing destruction or transfer to NARA, unless subject to a legal hold.

13.7. Destruction of Records

13.7.1. Destruction Restrictions

Permanent Case Files: Previously, and pursuant to criteria outlined in the Records Retention Plan, the RMD issued instructions to the field on the procedures for identifying and stamping certain field office paper files / records with legends "DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES" and/or "X: DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES." Paper files so stamped are permanent and must be retained for eventual transfer to NARA. It is no longer necessary to continue this practice of stamping files.

FOIPA Requests: Upon receipt of a FOIPA request, a search is conducted by the RMD's Record / Information Dissemination Section (RIDS) for responsive records. RIDS marks relevant files to indicate a FOIPA request was received for the file. Files are marked by inserting a 17-1 Form as the top serial in each section, subfile, bulky or enclosure behind file (EBF) prior to those items being sent to DocLab for electronic conversion. This precludes premature destruction of the original paper files prior to resolution of the FOIPA request.

Legal Holds: See Legal Hold Corporate Policy Directive 0619D

Auxiliary/Lead Office Files: Field offices are authorized to review their auxiliary/lead office files to identify material eligible for destruction or transfer to the OO. Auxiliary/Lead offices should identify original material and forward it to the OO for inclusion in the OO's case file. Examples of documents which should be removed from the auxiliary/lead office file and transmitted to the OO include: Original FD-302s, laboratory reports, latent fingerprint reports, original surveillance logs, SAs' investigative notes, original photographs and other original documents maintained in the 1A section of lead office case files. Refer to the Disposition of Auxiliary/Lead Office files for more information.

13.7.2. Documenting Records Destruction

To document the destruction of records whose case information is not recorded in ACS or Sentinel, record the file number and date of destruction on a Form FD-478 (List of Files Destroyed / Transferred to FBIHQ). Form FD-478, containing the file numbers and the dates files were destroyed, is maintained at the beginning of each respective classification in the closed files section. Since the destruction of ACS and Sentinel cases is recorded in ACS and Sentinel, it is not necessary to annotate the destruction of these files on an FD-478. Records may be destroyed only at the direction of the Records Disposition Unit (RDU).

13.7.3. Destruction of Field Office Records

Offices must retain closed investigative and intelligence case files until the RDU issues guidance providing specific disposition instructions or directs the transfer of records in a specific file classification to FBIHQ for processing and transfer to NARA.

Field offices may not destroy their records without specific authorization from the RDU. All time periods and cut-off dates for records destruction are established by the RMD and must be strictly adhered to without exception. See the Guidance to Field Offices web page for the most current listing of approved disposition actions to be utilized by field offices.

13.7.4. Disposition of Evidence/Property

Certain case files are marked with the notation "DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES" and are eventually transferred to NARA. In such instances, only those evidentiary and non-evidentiary exhibits, regardless of size, which are documentary in nature, generated by and considered FBI records (i.e., SA's interview notes, photographs, work papers, ledgers, journals, etc.), are preserved as part of the case file.

Documentary materials, such as records of private enterprises, original or copies, contributed, seized or subpoenaed, are returned to the rightful owner when the investigative or administrative purpose for which they were obtained has been satisfied. Likewise, physical property (such as typewriters, radios, televisions, firearms, etc.) is returned to the rightful owner or, if required, disposed of in accordance with approved procedures in the case of drug evidence, illegal firearms, forfeited and abandoned property, etc. Any evidence scanned by the RMD's DocLab and copied to a CD to aid in searching is destroyed following case closure. Evidence which is FBI-generated, such as chain-of-custody forms, crime-scene photographs, and laboratory analysis, is filed in the related investigative case file and assumes the retention period established for this file. See the Field Evidence Management Policy Guide 0780PG for more information.

13.7.5. Destruction of Index Records

Automated index/entity records will remain in the central recordkeeping system when the corresponding file is destroyed or transferred and will be marked accordingly. Copies of index records corresponding to permanent case files are provided to NARA along with the related case file. RMD digitized manual indices cards created prior to automation and provided electronic versions of the cards to NARA.

13.7.6. Destruction of Copies in Files

Duplicate copies of communications maintained within the same case file not containing action notations (i.e., notations issuing instructions, notations requesting action be taken, notations of certification action was taken, etc.), may be removed and destroyed when the case file is closed, unless subject to a legal hold. Copies of documents which

contain action notations not appearing on the original file copy are retained within the same case file along with the original file copy.

13.7.7. Destruction of Record Checks

Lead offices send the OO the results of contacts with various credit, law enforcement, and federal, state, and local agencies to determine criminal, credit, and/or employment status of individuals related to current investigations.

Record checks in the OO are retained / destroyed commensurate with the disposition authority of the OO case file to which the record check relates.

Field office files containing record checks conducted in connection with applications for employment, and resulting in receipt of information identifiable with the applicant may be destroyed in accordance with applicable disposition authorities or when all administrative needs have been met, whichever is later, unless subject to a legal hold.

13.7.8. Destruction of 67 File Classification (Applicant and FBI Personnel)

Copies of applicant records maintained by field offices and LEGATs must be destroyed when no longer needed, or in accordance with the applicable disposition authority, whichever is sooner, unless subject to a legal hold. Do not forward copies of applicant case files to the ARC or to another field office.

Case files where an appeal and/or litigation has been filed and which contain complaints with related correspondence, reports, exhibits, withdrawal notices, copies of decisions, records of hearings and meetings by the Equal Employment Opportunity Commission (EEOC) or the United States Court(s) may be destroyed after resolution of the case and in accordance with the applicable disposition authority.

For field office case files containing only correspondence and/or leads received from other field offices or FBIHQ, which supplements the full background investigation being conducted primarily by FBIHQ or another field office, all original documents must be sent to FBIHQ to ATTN: ARC-1. The duplicative material maintained within the field office files may then be destroyed when all administrative needs have been met.

Background investigators' raw notes used to prepare a final report (FD-302) may be maintained separately from the applicant case file. The raw notes may be destroyed in accordance with the applicable disposition authority, as long as the final report has been incorporated into either the personnel file or unsuccessful applicant's case file.

13.8. Disposition of Administrative Records - Classifications 319, 67Q and Legacy 66

Most of the FBI's administrative records have temporary retention periods. This means after a certain period of time has elapsed, the records can be destroyed or deleted, unless subject to a legal hold. As previously stated, administrative records include

budget, time and attendance, supply, and other housekeeping functions common to all federal government offices.

13.8.1. Disposition of Administrative Records in Sentinel

Sentinel automates the disposition application for administrative records uploaded or created in Sentinel or migrated from ACS. Sentinel tracks the record's retention, provides notice of disposition eligibility, and then facilitates disposition, unless subject to a legal hold. Previously, partial destruction of discrete blocks of hard copy records which met their retention requirements was performed in each office with RDU coordinating the deletion from ACS. Partial destruction, as it was applied previously, is no longer an active process in Sentinel. Although Sentinel automatically flags record material for disposition it does not automatically dispose of it. The procedure for this operation is currently under development by the Sentinel Program.

13.8.2. Disposition of Paper Administrative Records

Administrative records not retained in Sentinel will continue to have disposition applied manually. To facilitate destruction, these administrative records are closed or cut-off at regular intervals, normally at the close of a fiscal or calendar year. This cut-off permits the segregation of an accumulation of related records in a discrete block. At the end of a specified time period, all records in the block are destroyed or deleted, barring any legal holds or other actions which would temporarily extend the retention period. Offices may destroy or delete these records by applying the disposition instructions approved for Classification 319 Guide and Classification 67Q Guide records without receiving additional instruction from the RMD, unless subject to a legal hold.

13.8.3. Disposition of Legacy Classification 66

The implementation of the administrative Classifications 319 and 67Q replaced the administrative Classification 66. This legacy classification is no longer used except for Bureau Automotive Accidents opened in 66A. Existing Classification 66 case files, kept in hard copy, are eligible for disposition when the file, in its entirety, aligns with an approved 319 and 67Q disposition and has met its retention, unless subject to a legal hold. Offices should review their Classification 66 case files for possible disposition.

13.9. Destruction of Copies of Records

Offices routinely print reference copies of ECs, e-mail messages, and other records. 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 copies and non-record materials may be destroyed or deleted when no longer needed for reference purposes, unless subject to a legal hold.

Annually offices should review non-record materials, including e-mail stored in electronic folders or inboxes, and destroy or delete any materials which are superseded or are no longer useful, unless subject to a legal hold.

13.10. **Destruction of Draft Documents**

Working files, such as preliminary drafts and notes, and other similar materials, should be destroyed or deleted when the final documents have been approved by the FBI official with authority to do so unless they:

- Are subject to a legal hold
- Relate to pending Freedom of Information and Privacy Acts (FOIPA) requests.
- Have some other business reason requiring retention for reference purposes

Within the FBI, drafts remaining from past actions and cases should be deleted or destroyed when consistent with this policy. Similarly, documents never achieving final status or on which actions are stopped should be destroyed / deleted regularly, consistent with this policy. This guidance does not supersede the requirement for original notes of interview with prospective witnesses and/or suspects and subjects to be retained in the 1A section of the case file. See Section 3.3.1.1.4 of the Domestic Investigations and Operations Guide 0667DPG.

This guidance applies to all drafts created in any media, unless draft documents are specifically addressed in the records retention schedule for a records series. This includes copies of drafts appended to e-mail or stored on removable media, any computer, or network drive or in hard copy. Marking documents as drafts avoids confusion and alerts others the document has not been finally approved.

13.11. **Destruction of Personal Files**

Personal papers are materials which belong to an individual and are not used to conduct FBI business. They are primarily personal in nature and may be in any format or media. Examples of personal papers include an employee's copy of his or her SF-50 or an e-mail inviting co-workers to an anniversary celebration. It is important to note if a document contains both record and personal information, the document must be treated as a record.

According to NARA, personal files may include materials accumulated by an individual before joining the FBI not later used to conduct government business. Examples include previous work files and reference files. Personal files may also be items relating solely to an individual's family matters, outside business pursuits, professional activities, or private political associations. Examples include family and personal correspondence, volunteer and community service records, or literature from professional organizations.

Personal files should be clearly designated and maintained separately from official FBI files. These materials can be destroyed when no longer needed.

13.12. **Emergency Destruction of Records**

Under certain conditions, records are destroyed if they constitute a continuing menace to human health or to FBI property. Records exposed to radiological, biological or chemical agents, or otherwise contaminated or infested, are immediately reported to the RMD. Other circumstances warranting early destruction of records include wartime or other national emergency conditions. The RMD requests approval for emergency destruction of the records from NARA. Upon receipt of NARA's concurrence, the RMD will coordinate the appropriate means of destruction and generate a report describing the records and the circumstances of their destruction. See 36 C.F.R. § 1229 for more information on emergency destruction.

13.13. **Orphaned Records**

Orphaned records are records left behind by their creators. An example includes records abandoned in offices after FBI personnel have moved to another office or left the Bureau. FBI personnel must be aware of their responsibilities in ensuring the records in their custody are not inadvertently left behind during office moves or departures.

If orphaned records are found, the finder should:

a) Keep all files, binders, folders, photographs, tapes, diskettes, CDs, etc., in the same box or filing cabinet and in the same original order; do not disassemble any of the files;

b) Look through the files to obtain names, organizations, telephone numbers, or any other information which might help identify the owner or someone familiar with the files;

c) Try to determine what the files contain; if they contain any security classified materials; if the materials relate to a particular case or investigation; if they appear to be copies; the dates of the files; and

d) Place a sheet of paper in the box or on front of the file cabinet indicating 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:

a) Owner: Contact 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 a manager of the unit/section/division. If an owner is located, arrange to transfer the records to the owning office. Document the transfer in an EC or e-mail message.

b) Case Files: Search Sentinel to determine if the record has been imported and serialized into a case. If the record is contained in Sentinel, then it is a copy and

can be destroyed. If the record is not contained in Sentinel, it should be sent to the case owner for importing.

c) ECs: Search for any ECs in the files. Search Sentinel to determine if the EC has been imported.

d) Administrative records: Determine 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 orphan file material. If so, apply the 319 and 67Q disposition instruction.

e) 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.

f) Evidence: Check if there are photographs or other items marked evidence. Try to determine with which case the evidence is associated. If possible, contact the applicable office to see if you can return it. If needed, contact the Evidence Program Office at the Laboratory for more information.

g) Personal information: Check if the records contain personal information about FBI personnel. If so, return the records to the supervisor of the unit to which the FBI personnel reports. If the material is of a truly personal, private nature, and therefore not a record, return the item directly to the FBI personnel.

h) Personal belongings: Check if the box/filing cabinet contains personal belongings. If possible, contact the individual to who the materials belong and arrange to return the belongings.

i) Maps and drawings: Check if the files contain commercially available maps or illustrations. These items may be destroyed unless an owner is discovered.

j) Binders and other presentation materials: 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 may be destroyed.

k) 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 which are captured elsewhere in the official files, then the magnetic devices may be destroyed.

14. Identifying and Managing Historical Records

Almost every investigative and intelligence file classification contains some non-transitory records which have been designated as permanent by NARA. The RDU works with NARA to identify these permanent non-transitory records and protect them as part of the historical documentation of the FBI's activities.

14.1. Transfer of Permanent Non-Transitory Records to NARA

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

Prior to the transfer of historical records to NARA, the RDU requests the assistance of the RMD's Declassification Review Unit to review closed case files or records in certain file classifications exempt from automatic declassification. The Declassification Review Unit reviews the material and either identifies it for continuing classification or declassifies it. Lastly, RDU updates records with a notation the file has been accessioned to NARA.

14.2. Transfer of Permanent Non-Transitory Electronic Records

Although most FBI electronic information systems do not yet have disposition authorities, some of the systems contain permanent or potentially permanent electronic records. The transfer of electronic records is similar to the transfer of paper case files. The RDU transfers the records in accordance with disposition instructions as well as any additional requirements NARA has established for the transfer of electronic records.

15. Unauthorized Destruction of FBI Records

FBI personnel are responsible for preventing the unauthorized destruction, damage, or removal of records. Records must not be destroyed or removed from the legal custody of the FBI except in accordance with authorized dispositions. Any unauthorized destruction should be reported to the 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.

Appendix A: Sample File Plans

Sample File Plan – Paper Records

FILE PLAN			
1. Office: Gordon Point Field Office Squad 8	2. Phone: 303 555 1234	3. Rm. No.: 334	4. For FY: 2013
5. Prepared by: John Doe, File Supervisor	6. Approved by Jane Doe		7. Date: 09/30/2012

Classification or File Series Number	Case File Number	Classification or File Series		Location	Disposition Instructions
		Title	Description		
67Q44	No file number has been assigned.	Supervisor's Drop File		Supervisor's Office	Review annually and destroy superseded or obsolete documents.
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.
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.
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.

Sample File Plan – Electronic Records

The sample file plan below is used to manage files maintained in electronic form on a shared drive. The file plan should be saved on the shared drive in a folder entitled "File Plan."

Any documents created or used in the course of business must be stored on the shared drive in the appropriate file category. This may be done by saving the document to the appropriate shared drive folder. Documents should only be deleted from the shared drive in accordance with the file plan.

File Category	File Description	Disposition
242	**Electronic Recordkeeping Certification of FBI Systems** (Contains the following): 242 - Electronic Recordkeeping Certification (ERKC) 242 - [redacted] b7E 242 - RMD IT Management 242 - SENTINEL 242 - SENTINEL & Virtual Case File 242 - Trilogy	Not authorized.
278	**Quarterly PIOB Reports for the Unit** Copies of responses and Supporting Documentation Maintained by Divisions and Offices.	Temporary - Destroy after the next canvass cycle.
319D2	**Records Management Application Unit (RMAU) Budget Preparation and Presentation** Matters related to the budget of the unit (Contains the following): 2009 Budget 2010 Budget 2011 Budget 2012 Budget 2013 Budget	Destroy when 6 yrs 3 months old.

319O3	**Records Disposition Background Material** Descriptive inventories, disposal authorizations, schedules, and reports.	Destroy 6 years after the related records are destroyed or after the related records are transferred to the National Archives of the United States, whichever is applicable.
319O11	**Records Management Correspondence and Reports** The file contains other correspondence and reports. This category does not include anything which establishes policy. Policy documents are maintained in 319W2 files. This category also contains a subfolder for the website.	Destroy when 6 years old.
319O24	**Inspection and Audit Records** Copy of self inspection reports (within RMD) and reports received from the Inspection Division regarding RMAU programs and processes.	Destroy following the next audit or when 7 years old, whichever is later.

319T1	**Office Administration** Records accumulated by individual offices which relate to the internal administration or housekeeping activities of the office rather than the functions for which the office exists. In general, these records relate to the office organization, staffing (night and weekend schedules), procedures, and communications, including facsimile machine logs; the expenditure of funds, including budget records; day-to-day administration of office personnel including training and travel; supplies and office services and equipment requests and receipts; and the use of office space and utilities. They may also include copies of internal activity and workload reports (including work progress, statistical, and narrative reports prepared in the office and forwarded to higher levels) and other materials which do not serve as unique documentation of the programs of the office. (Contains the following): 319T1 - Comments on Policy Documents 319T1 - Comments on Inspections of Other Offices 319T1 – Copier Usage Report 319T1 – Copies of RMAU Travel Vouchers 319T1 – Personnel Counts 319T1 – Activity Reports 319T1 – Office and Space Management 319T1 – Personnel Administration Records 319T1 – Security Reports 319T1 – Training Files	Destroy/delete when 2 yrs old.
319U18	**Information and Technology Management** IT Infrastructure Design and Implementation (Contains the following): 319U18 - IT Life Cycle MGMT 319U18 - IT Strategy & Planning 319U18 - Records Enterprise Architecture	Records for projects which are implemented: Destroy/delete 5 years after project is terminated. Note: Records for projects which are not implemented should be destroyed within one year after final decision is made.

319W2	**Administrative Policies Written by the Office** This file contains the policy and procedural documentation for internal housekeeping and operational activities unrelated to the Bureau's mission. A copy of all drafts should be maintained until finalization of the policy, procedures, guidance, or technical manual, but may be destroyed at this point (IAW N1-065-06-13, item 1).	PERMANENT. Transfer to NARA in 5-year blocks when the newest record is 5 years old.
319X6	**Submissions to the Mission and Function Statements** Office input into the final version of the FBI's mission and function statements.	Destroy when 5 years old.
319Y5	**External Committees and Boards** Organized in folders by name of board/committee, such as ARMA, AIIM, FIRM, NARA, etc. For very active files with large volumes of material, the files can also be divided by fiscal year for activities of a particular board	Destroy when 3 years old.
319Y5	**Internal Committees and Boards** Organized in folders by name of board/committee, such as EAB, TRB, IMPRB, ITRRWG, etc. For very active files with large volumes of material, the files can also be divided by fiscal year for activities of a particular board (such as has been done with the EAB files).	Destroy when 3 years old.

Appendix B: Key Words

ACS: Automated Case Support system; a centralized case management system used by the FBI from October 16, 1995, to June 30, 2012, to electronically file and disseminate case files. On July 1, 2012, ACS was replaced by Sentinel. ACS is made up of three components:

- **ICM:** Investigative Case Management, was used to open cases and to maintain cases, leads, and ticklers
- **ECF:** Electronic Case File was used to maintain, track, and disseminate documents, by assigning unique serial numbers to each document
- **UNI:** Universal Index continues to be 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 government business which is complete and accurate to the extent required to document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and 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: Document day-to-day organizational and/or housekeeping activities such as those related to budget, time and attendance, supply, or similar functions which are created by all units at the FBI during the course of normal business. Administrative records are not related to the unique mission or programs of the FBI. Examples of housekeeping records can be found Classification 319T, Records Common to Most Offices, and Classification 67Q, Personnel Matters. An example of organizational administrative records can be found in Classification 319X, Organizational Records and Supporting Documentation.

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

Attribute: A distinct characteristic of an object.

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
- **Administrative Case Files:** Document specific matters related to facilitative functions, such as human resources, budget, or transportation; when referring to

an administrative file the letter "A" must be included with the file number (e.g., 242-HQ-A123456 or 319C-HQ-A123456)

- **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.

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

Chronological Files: Files arranged by date.

Classification: As used in this manual, classification refers to the category of investigative or administrative case files. Classification also means the designation of a national security classification level.

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.

Correspondence: Letters, memoranda, notes, electronic mail, or 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: Action taken after a record is no longer needed by the agency for normal business purposes. This includes destruction or transfer of permanent records to NARA.

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).

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

Electronic Communication (EC): Includes e-mails, text messages, instant messages, voice mail, pin-to-pin communications, social networking sites, bulletin boards, blogs, and similar means of electronic communication.

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

Electronic Mail (e-mail): Documents created and sent or received on an e-mail system, including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents which may be transmitted with the documents. E-mail messages may be sent or received via the UNET, FBINet, SCION, or any other FBI-operated e-mail system.

Electronic Mail (e-mail) System: A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities, data systems used to collect and process data which have been organized into data files or databases on either personal computers or mainframe computers, and electronically generated documents not transmitted on an electronic mail system.

Electronic Messages: Electronic mail and other electronic messaging systems used for purposes of communicating between individuals.

Electronic Messaging Account: Any account that sends electronic messages.

Electronic pointer or reference: Pointers or references in non-record automated systems which serve to direct the user to the FBI's central recordkeeping system. These include, for example, documents uploaded to ACS, which are not official records but serve as a reference and pointer to the official record.

Electronic records: Any information recorded in a form only a computer can process and which satisfies the definition of a Federal record under the Federal Records Act. The term includes both record content and associated metadata the agency determines is required to meet agency business needs. (36 C.F.R. § 1220.18).

Electronic Recordkeeping Certification (ERKC): Mandatory comprehensive evaluation of the technical and non-technical electronic records management features of a system, to determine whether the system satisfies electronic recordkeeping criteria.

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

Enclave: A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Evidence: Information which is legally submitted to a competent tribunal as a means of ascertaining the truth of any alleged matter of fact under investigation before it. Also, anything a suspect leaves at a crime scene or takes from the scene or may be otherwise connected with the crime. Physical, real, tangible, laboratory, and latent are all adjectives to describe the types of evidence the FBI Laboratory Division examines.

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 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.

FBI executives: Those serving in the position of Executive Assistant Director or above.

FBINet File/Print Server ("Secret" enclave): Servers which manage all files and print services in the FBINet infrastructure.

Federal Records Act: Codified at 44 U.S.C. § 3101 *et seq.*, amended in 1950. An Act which 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: An accumulation of records or non-record materials arranged according to a plan or a unit, such as a paper or electronic folder, containing records or non-record materials.

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

File Number: Consists of a classification number indicating the general category of the case, an alpha designator for subcategories within the classification, a two-letter designation for the Office of Origin (OO), and a case number automatically created and assigned sequentially by the central recordkeeping system (currently Sentinel). An example of a file number is 91A-BA-1234576.

File Plan: A plan designating the physical location(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.

File transfer utilities: Software which transmits files between users but does not retain any transmission data.

Freedom of Information Act (FOIA): Codified at 5 U.S.C. § 552, enacted in 1966. An Act which provides access to federal records, except for those records protected from public disclosure by exemption or exclusion.

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

Full Data Backup: Electronic copy of all user data to include date created, date modified, and date last used.

GRS (General Records Schedule): Issued by the Archivist of the United States; GRSs authorize, after specific periods of time, the destruction of temporary records or the transfer to NARA of permanent records which are common to several or all agencies. In the FBI, one of the GRSs has been incorporated as Classifications 319 and 67Q.

Importing: The process of uploading digital files into Sentinel via the Sentinel Import Form (FD-1036).

Information Management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to the organized collection, processing, transmission, and dissemination of information.

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

IT Systems Administrators: Personnel with oversight authority over information technology equipment and processes.

Key custodian: The person to whom a legal hold notice is directed. The key custodian holds or is in charge of overseeing and maintaining potentially relevant information related to a lawsuit whether stored in electronic or paper format.

Legal Hold: The procedure for locating and ensuring the retention of paper and electronic information subject to a preservation obligation.

Lifecycle: The concept which records pass through several stages, which are creation, maintenance and use, and disposition.

Medium: The physical format of a record; examples include paper, electronic, video/audio tapes, micrographics, and other materials on which information can be recorded.

Metadata: Data describing information; in particular, its context, content, and structure and its management through time.

National Archives and Records Administration (NARA): The U.S. Government agency responsible for the maintenance and management of all federal records.

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

Non-transitory record: A non-transitory record is a record needed for more than 180 days which has one or more of the following characteristics: (1) provides substantive documentation of the FBI's policies and actions, (2) contains important and/or valuable evidentiary information, and/or (3) is required to be maintained by law or regulation. A non-transitory record may have a permanent or temporary retention requirement.

Office of Origin (OO): 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 the case. All of the actions reported on the case are serialized and uploaded into the one OO number for the case, even if other divisions/offices are creating and serializing the documents. The DIOG, Appendix J contains guidance regarding the determination of the office of origin.

Official Personnel Folder (OPF): A group of records, relating to one employee as identified in OPM's "The Guide to Personnel Recordkeeping." The FBI recently implemented the eOPF, which makes an employee's entire OPF, with the exception of medical, security, and financial records, available to the employee online. An employee's medical, security, and financial records continue to be maintained in hard copy at the ARC.

Performance Appraisal Report: A document containing the performance evaluation of each employee based on the Critical Elements outlined in the employee's Performance Plan.

Performance Plan: A document provided to FBI personnel describing the Critical Elements and the performance standards used to rate performance. The Performance Plan will vary depending on the Job Family and Performance Level as well as the optional Specialized Critical Elements.

Performance-related Information / Documentation: Any material gathered, prepared and/or maintained by the FBI personnel's team leader, supervisor, rating official, and/or reviewing official, for the exclusive purpose of evaluating the FBI personnel under the FBI performance appraisal system. Performance-related Information / Documentation includes but is not limited to, the Performance Appraisal Report and the Performance Plan, positive and negative performance feedback and FBI personnel's self-assessment.

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 approximately 25 years after closing.

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

Personally Identifiable Information (PII): Any information which can be used to distinguish or trace an individual's identity such as a name, social security number, or biometric record either by itself or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

Personnel: Any individual employed by, detailed, or assigned to the FBI, including members of the Armed Forces; an expert or consultant to the FBI; an industrial or commercial contractor, licensee, certificate holder, or grantee of the FBI, including all subcontractors; a personal service contractor of the FBI; or any other category or person who acts for or on behalf of the FBI, as determined by the FBI Director.

Personnel folder: An unofficial file maintained to house the performance-related information / documentation; this is equivalent to a supervisor's drop folder and should not be confused with the official personnel folder (OPF).

Privacy Act: Codified at 5 U.S.C. § 552a; enacted in 1974. The Privacy Act regulates the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

Program Records: Records which document the unique, substantive functions of the Bureau, in contrast to administrative records. Program records may be referred to as mission-related records; they are created by, among others, White Collar Crime, Violent Crimes, Cyber, Language, and Security.

[redacted] b7E

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 electronic system which captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.

Records: All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Records do not include library or museum material made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes

all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (44 U.S.C. § 3301).

Records Audits: Independent review and examination of records and activities to test for compliance with established policies and standards, often with recommendations for changes in controls or procedures.

Records Inventories: A detailed listing including the types, locations, dates, volumes, equipment, classification systems, and usage data of an organization's records in order to evaluate, appraise and organize the information.

Records Liaison: An individual designated by the Division/office who facilitates the coordination of records management issues at the Division/office level.

Records Management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations.

Records Management Application (RMA): A software application which 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.

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

Records System (Official): A records system, which may also be called a "records management system," is a system capable of properly managing data and/or records.

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. A document providing disposition authority for one or more series of records.

SCION: Sensitive Compartmented Information Operational Network (SCION) is the network which connects the FBI to the Intelligence Community (IC) via the Joint Worldwide Intelligence Communications System; SCION also provides capabilities for

analysts to access raw intelligence and intelligence products, perform analysis, and distribute intelligence products with its IC partners.

Sentinel: Implemented on July 1, 2012; Sentinel is the FBI's official electronic recordkeeping system. It is an automated system in which records are collected, organized, and categorized to facilitate their retrieval, use, and disposition. Sentinel provides a web-based environment for creating, collaborating, approving, and distributing FBI information. Sentinel provides enhanced search and analysis capabilities and facilitates information sharing with law enforcement and intelligence community members, including the Departments of Justice and Homeland Security.

Serial: Documentary material placed in case files and numbered sequentially.

Serializing: The automatic numbering of a document, to include the document's attributes, into an FBI electronic information system, such as Sentinel.

Technical Reference Files: Non-record copies of regulations, publications, articles, or other materials 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 Record: A temporary record which has only minimal documentary or evidentiary value and is needed for 180 calendar days or less.

Unauthorized disposition: The unauthorized destruction, removal, or mutilation of federal records.

Uploading: The process of sending data (text of document) electronically into an electronic information system; in the context of Sentinel, digital files are uploaded, or imported, into Sentinel via the Sentinel Import Form (FD-1036).

Vital Records: Vital records are essential to the functions of the FBI's operation during and following an emergency. The loss of these records during a disaster could create gaps in vital information resulting in the disruption of essential services, exposure to unplanned expenses of financial settlements or loss of revenue, increased vulnerability to litigation and loss of productivity.

Vital Records Officer: Identifies and maintains vital records in accordance with established requirements; provides training on vital records policies and procedures for

division personnel; and coordinates with the RMD, at least annually, to develop an action plan for the protection of vital records.

Working Files: Records accumulated as part of a work process but not necessarily having a place in the case file or other official file are working files. 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