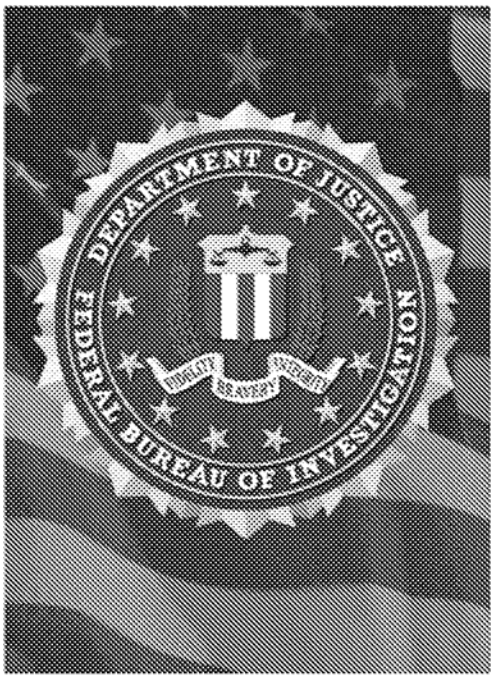
Records and Information Management Policy Guide



Federal Bureau of Investigation

Information Management Division

1223PG

September 22, 2022

Approvals

Policy Information	
Last Updated	N/A
Effective Date	2022-09-22
Approval Information	
Sponsoring Executive Approval	**Arlene A. Gaylord** Assistant Director Information Management Division
Final Approval	**Brian C. Turner** Associate Deputy Director

General Information

Questions or comments pertaining to this policy guide can be directed to:

Federal Bureau of Investigation Headquarters (FBIHQ), Information Management Division (IMD)

Division point of contact: IMD Help Desk [redacted]

Supersession Information

This document supersedes: *Records Management Policy Guide* (0769PG); Records Management User Manual; *Vital Records Policy Guide* (0794PG); *Records Management Requirements for the Creation, Maintenance, and Decommissioning of SharePoint Sites Policy Directive* (0768D); *Records Management Standards for Scanned Documents Policy Directive* (0774D); *Records Management Scanner Equipment Standards (Including Document Conversion Laboratory Services Requirements) Policy Directive* (0786D); *Preservation of Federal Bureau of Investigation (FBI) Executive Records (Executive Assistant Director, EAD, and Above) Policy Directive* (0949D); *Expungement of FBI Records from Investigative Case Files Policy Directive* (1014D); and [redacted] b7E

This document is a new publication; no previous versions are available.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit listed in the contact section of this policy guide.

Revision Log

The revision log documents substantive changes made to the previous version of this policy. The numbers and titles in the "Revised" column refer to the subsections as they currently appear in this updated policy. "Deleted" subsection numbers refer to those in the previous published version of the policy.

Revised Section Number and Title	Deleted Section Number and Title
Significant changes have been made throughout this policy.	

Table of Contents

1. Introduction 1
1.1. Purpose 1
1.2. Scope 1
1.3. Exemptions 1
2. Roles and Responsibilities 2
2.1. The Director 2
2.2. Information Management Division 2
2.2.1. Assistant Director 2
2.2.2. Agency Records Office 2
2.2.3. Mission Support Services (MSS) 3
2.2.4. Information Services Section (ISS) 4
2.2.5. Record/Information Dissemination Section (RIDS) 4
2.2.6. Technology Innovation Section (TIS) 5
2.2.7. Enterprise Vetting Center (EVC) 5
2.2.8. Essential Records Program (ERP) Manager 6
2.3. Security Division (SecD) 6
2.3.1. Continuity of Operations Coordinators and Chief Security Officers (CSO) 6
2.3.2. Information System Security Officers (ISSO) 6
2.4. Office of the General Counsel 7
2.4.1. DGC of the Investigative and Administrative Law Branch (IALB) or the National Security and Cyber Law Branch (NSCLB) 7
2.4.2. Litigation Branch (LitB) 7
2.5. Information and Technology Branch 7
2.5.1. Information Technology Applications and Data Division (ITADD) 7
2.6. Criminal Justice Information Services (CJIS) Division 8
2.6.1. CJIS, Biometric Services Section (BSS), Criminal History Information and Policy Unit (CHIPU) 8
2.7. FBI Senior Officials (Director, Deputy Director [DD], Associate Deputy Director [ADD], and Executive Assistant Directors [EAD]), or their designees: 8
2.8. FBIHQ Divisions, Field Offices, and Legal Attaché Offices 8

2.8.1. ADs, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), and Legal Attachés (LEGAT) 8
2.8.2. Records Liaison (RL) 9
2.8.3. Information Asset Manager (IAM) 9
2.8.4. System Owners (i.e. Program Managers and Business Owners) 10
2.8.5. SharePoint site owners, content managers, and content administrators 10
2.8.6. Essential Records Officers (ERO) 10
2.9. FBI Personnel 11
3. Policy Statement 13
4. Processes and Procedures 14
4.1. Records and Information Management 14
4.1.1. Types of Records 14
4.1.2. Types of Nonrecord Information 16
4.2. Records Receipt and Creation 18
4.2.1. Records Receipt 18
4.2.2. Records Creation 19
4.2.3. Electronic Records 25
4.3. Records Maintenance and Use 31
4.3.1. Records Series and Filing Locations 31
4.3.2. File Plan 31
4.3.3. Case File Classification and File Types 32
4.3.4. Management of Classification 319 and 67Q Files 33
4.3.5. Short-Term Temporary Administrative Records 34
4.3.6. Personnel Records 34
4.3.7. FBI Senior Official Records 35
4.3.8. File Request System (FRS) 36
4.3.9. Case File Management 37
4.3.10. Hard Copy Case Files 40
4.4. Records Disposition 44
4.4.1. Records Scheduling 44
4.4.2. Records Retention Plan 44
4.4.3. Creating New Records Series 45
4.4.4. File Cutoff and Retention Period 45

4.4.5. Disposition 46
4.5. Records Protection and Records Recovery Program 49
4.5.1. Records Protection 49
4.5.2. Records Recovery Program 52
4.6. Essential Records and the Essential Records Program 52
4.6.1. ERO Designation 52
4.6.2. Identifying and Protecting Essential Records 52
4.6.3. Contingency Planning and Risk Assessment 53
4.6.4. Essential Records Plans 53
4.6.5. Protection Methods 54
4.6.6. Training 57
4.6.7. Review and Testing 57
5. Summary of Legal Authorities 58

List of Appendices

Appendix A: References A-1
Appendix B: Definitions and Acronyms B-1

1. Introduction

Records and information are key resources of the FBI. Proper records and information management supports the full spectrum of the organization's mission, empowering better decision-making, ensuring institutional integrity, and promoting public trust.

1.1. Purpose

The purpose of this policy guide (PG) is to set forth the FBI's records and information management policies, requirements, and procedures as governed by applicable laws and regulations.

1.2. Scope

This PG applies to all FBI personnel and across all enclaves.

1.3. Exemptions

There are no exempted FBI personnel or programs.

2. Roles and Responsibilities

2.1. The Director

The Director of the FBI must:

- Ensure records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions are created and preserved.
- Delegate records management authority and responsibility for the essential records program to the Information Management Division (IMD) assistant director (AD).

2.2. Information Management Division

2.2.1. Assistant Director

The IMD AD must:

- Oversee the management of an FBI-wide records and information management program on all enclaves and in all media and formats.
- Designate an agency records officer (ARO) who is certified by the National Archives and Records Administration (NARA) and is responsible for developing and implementing agency recordkeeping requirements.
- Designate an essential records program manager to oversee the FBI's Essential Records Program.

2.2.2. Agency Records Office

The ARO must:

- Set forth and manage an Enterprise Information Management (EIM) strategy and cascading objectives across all enclaves and repositories through innovation, collaboration, and assistance from Information Technology Branch (ITB), the Office of the Chief Information Officer (OCIO), the Office of the General Counsel (OGC), FBIHQ program managers (PM), and field offices (FO) to realize the full value of the FBI's information assets.
- Develop the FBI's records and information management program and provide guidance to ensure compliance with requirements for records and information management, and determine record or nonrecord status, as set forth in federal law.
- Create and maintain recordkeeping policies for the enterprise and review other FBI policies to ensure adequate recordkeeping guidance is provided in accordance with records management laws and regulations; develop new and update existing records control schedules to ensure proper disposition of records in all media and formats.
- Serve as the IMD's primary liaison with FBIHQ divisions, FOs and Legal Attaché Offices (Legat) on records and information management matters; provide guidance on records and information management policies; and communicate with and provide guidance on new records schedules, file plans, policies, and procedures.

- Conduct audits to ensure records are created and maintained in accordance with policies and procedures.
- Collaborate with Security Division (SecD) on the identification and maintenance of essential records and advise FBI personnel on the management of essential records, including the storage and securing of essential records in support of the FBI's Continuity of Operations Program (COOP).
- In coordination and collaboration with information technology (IT) divisions, offices, and groups:
    - Plan and assist with updates to the enterprise records management application (RMA).
    - Ensure proper record and nonrecord management requirements are incorporated into the design and deployment of information management systems on all enclaves, including monitoring compliance with records and information management requirements.
        - Evaluate electronic records systems ensuring compliance with recordkeeping requirements in accordance with the *Electronic Recordkeeping Certification (ERKC) Policy Guide* (0800 PG).
        - Evaluate nonrecord information management systems ensuring compliance with the *Managing Nonrecord Information and Information Expiration Policy* (1075D).
    - Issue guidance to FBI SharePoint users, site owners, content managers, and content administrators regarding site content and records management responsibilities.
- Process requests for the creation of SCINet SharePoint sites and review requests for decommissioning SharePoint sites on all enclaves (SCINet, FBINet and UNet), as well as advise users, site owners, content managers, and content administrators regarding records and information management responsibilities in accordance with section 4.2.2.4 of this PG.
- Work closely with the Department of Justice's (DOJ) Senior Agency Official for Records Management (SAORM) and the NARA on records and information matters.
- Advise senior FBI officials on existing, new, or potential records management statutes, regulations, or other legal requirements impacting the FBI, as well as brief new senior FBI officials on the preservation requirements for FBI executive records.

2.2.3. Mission Support Services (MSS)

MSS must:

- Provide the IMD workforce with administrative, human resources (HR), health and wellness, financial management, and security program services, as well as training opportunities to include career and leadership development.
- Liaise with Finance and Facilities Division (FFD) to augment the safety, operations, and amenities of IMD facilities.

- Deliver records and information management training and assistance to FBIHQ divisions, FOs, and Legats.

2.2.4. Information Services Section (ISS)

ISS must:

- Develop and implement operational procedures for the enterprise concerning the creation, organization, storage, access, maintenance, preservation, and disposition of FBI records regardless of medium or format (physical or electronic) in compliance with this PG.
- Manage the storage, maintenance, and disposition of records in FBIHQ storage areas, both physical and electronic.
- Utilize and maintain the enterprise Records Management Application (RMA) for the maintenance and disposition of case files.
- In Sentinel or other recordkeeping systems, assist with or process records modifications, case file classification management, case consolidations, serial transfers, permanent charge outs, and expungement requests.
- Provide document conversion services (both imaging and optical character recognition) to ensure the efficient, accurate, and timely conversion of the FBI's hard copy records and other evidentiary documents to a searchable electronic format which meets the customer's needs for handling (e.g. chain of custody), color, resolution, and output medium; furnish guidance for the use of scanning services in accordance with section 4.2.3.3, as well as the conversion of analog media and digital data stored on various legacy and modern media into accessible and exploitable formats.
- Coordinate with departing senior officials or their designees, ITB or other stakeholder divisions to obtain the collection of hard copy and electronic senior official records, and maintain records until disposition in accordance with section 4.3.7.3.
- Execute expungements in coordination with Criminal Justice Information Services Division (CJIS) and OGC's Deputy General Counsel(s) (DGC) per section 4.3.9.6.1.
- Oversee the transfer of inventoried closed case files from FBIHQ divisions, FOs, and Legats to the FBI's Central Records Complex (CRC).
- Transfer permanent records to the NARA and destroy or delete temporary records which have met their retention periods.
- Manage the Records Recovery Team of trained IMD personnel assembled to assist FBIHQ divisions, FOs, and Legats with pre- and post-disaster records assistance to include remediating, preserving, and mitigating the loss of records and when possible, restoring original records to a useful condition.

2.2.5. Record/Information Dissemination Section (RIDS)

RIDS must:

- Plan, develop, direct, and manage responses to requests for FBI information in accordance with the requirements of the Freedom of Information Act (FOIA) (United States Code [U.S.C.] Title 5 Section [§] 552); the Privacy Act of 1974 (5 U.S.C. § 552a);

Executive Order (EO) 13392, *Improving Agency Disclosure of Information*; EO 13526, *Classified National Security Information*; and other applicable Presidential, Attorney General, and FBI policies, procedures, and other mandates, judicial decisions, and Congressional directives.

- Coordinate with OGC regarding specific FOIA requests.
- Conduct declassification reviews of FBI information.
- Manage the prepublication review program.

2.2.6. Technology Innovation Section (TIS)

TIS must:

- Deliver information technology solutions to support IMD operations.
- Provide customer-focused, technology-based services through infrastructure support and application development.

2.2.7. Enterprise Vetting Center (EVC)

The EVC is the FBI's center of vetting excellence, providing timely, accurate, and actionable information to internal and external partners to stay ahead of the threat. It is comprised of the Foreign Threat Tracking Task Force and the National Name Check Program.

2.2.7.1. Foreign Threat Tracking Task Force (FTTTF)

FTTTF must:

- Protect the Homeland by coordinating with law enforcement, the United States intelligence community (USIC) and the National Vetting Center (NVC) to identify and prevent potential national security and criminal threats posed by individuals seeking entry into the United States via immigration process, including refugee, visa, and visa waiver program.
- Collaborate with field offices, Legats, and HQ divisions regarding operational needs related to individuals undergoing immigration vetting.
- Conduct thorough analyses of FBI holdings to determine whether a [redacted] will be issued for adjudication by its federal partners. b7E

2.2.7.2. National Name Check Program (NNCP) Section

NNCP must:

- Process name check requests submitted by federal agencies for the purposes of granting immigration benefits, making employment suitability determinations, and granting privileged access to a government facility, a government official, or to sensitive information.
- Provide useful, accurate, and comprehensive information to enhance our federal partners' ability to assess risks for the purpose of protecting the American people.
- Coordinate the release of FBI information from pending, restricted, and prohibited matters with respective field offices and HQ Divisions.

- Coordinate with the Office of the General Counsel (OGC) regarding specific name check requests.

2.2.8. Essential Records Program (ERP) Manager

ERP manager must:

- Serve as the IMD's essential records officer (ERO) and the FBI-wide ERO in connection with the Continuity of Operations Program (COOP) in accordance with section 4.6 of this PG.
- Establish and disseminate procedures governing the development, coordination, and overall management of the ERP and ensure consistency with FBI policy, federal regulations and guidelines.
- Oversee and coordinate with EROs on the management of essential records before, during, and after emergencies or disasters.
- Establish, train, and maintain a network of the EROs in all FBIHQ divisions and FOs.
- Provide essential records program information at SecD's Critical Mission Assurance Unit (CMAU) events and exercises.

2.3. Security Division (SecD)

2.3.1. Continuity of Operations Coordinators and Chief Security Officers (CSO)

COOP coordinators and CSOs must:

- Work with members of SecD to ensure the chosen alternative operating facilities possess, or are engineered to possess, security measures appropriate to the classification levels of the records stored within them.
- Coordinate with FBIHQ division and FO EROs to assess possible threats and risks to records to determine the level of protection or response required.
- Certify lists of essential records and method of protection for their respective FBIHQ divisions and FOs to ensure essential records have been reviewed and updated annually in accordance with section 4.6.
- Validate the availability of FBIHQ divisions' and FOs' essential records during COOP exercises to ensure essential records are retrievable and sufficient to operate during a COOP event.

CSOs must submit a Security Incident Report (SIR) via the enterprise process automation system (EPAS) for any missing hard copy or electronic files or serials which contain classified material or personal identifying information (PII) and reported by FBI personnel within their respective office. After submitting a SIR, CSOs must report the missing hard copy or electronic file or serial to the CSO Program Management Unit (CPMU) for further handling.

2.3.2. Information System Security Officers (ISSO)

ISSOs must provide guidance to EROs regarding the secure storage and protection of electronic essential records, when requested. In the absence of an ISSO, an FBIHQ division or FO CSO may be contacted.

2.4. Office of the General Counsel

2.4.1. DGC of the Investigative and Administrative Law Branch (IALB) or the National Security and Cyber Law Branch (NSCLB)

The DGCs of IALB or NSCLB or their designees must provide guidance to ISS on the expungement of information contained within investigative case files, in accordance with section 4.3.9.6.1 of this PG.

2.4.2. Litigation Branch (LitB)

2.4.2.1. Litigation and Technology Management Section (LTMS)

LTMS must:

- Assist with the expungement of information from employee personnel records in accordance with section 4.3.9.6.
- Provide guidance to FBI SharePoint users, site owners, content managers, and content administrators regarding SharePoint content, privacy, and e-Discovery responsibilities, and conduct decommissioning reviews and approvals in accordance with section 4.2.2.4. LTMS must consult with OGC's Privacy and Civil Liberties Unit (PCLU), as appropriate, on privacy-related matters.
- Assist FBI personnel with the adjudication and dissemination of record information in conjunction with the expungement of FBI records.
- Notify system owners when there is a need to retain the data backup for an electronic information system (e.g. Sentinel) beyond the standard retention period. LTMS must also notify system owners when an exception to the approved retention period has expired.

2.5. Information and Technology Branch

The ITB must:

- Collaborate with IMD to ensure new and existing IT systems, services, or equipment (e.g. scanners) which may create or store data, information, or records, have adequate record and nonrecord controls to ensure the complete lifecycle of these items are managed in compliance with federal law.
- Work with IMD to collect FBI senior officials' records from electronic repositories across all enclaves and transfer or maintain collected records in an agreed-upon format within 180 days of the senior official vacating the position, in accordance with section 4.3.7.3.

2.5.1. Information Technology Applications and Data Division (ITADD)

ITADD must:

- Provide approval or denial of SharePoint site requests, create new SharePoint sites upon approval, and decommission sites in coordination with SecD, OGC, and IMD pursuant to section 4.2.2.4.

2.6. Criminal Justice Information Services (CJIS) Division

2.6.1. CJIS, Biometric Services Section (BSS), Criminal History Information and Policy Unit (CHIPU)

The CJIS BSS, CHIPU must forward copies of redacted criminal history record information and certified court orders requiring the expungement of records from the FBI's central records system pursuant to the CSA, pretrial diversion, or other federal laws (these documents together make up an expungement notice) to IMD, in accordance with section 4.3.9.6.1.

2.7. FBI Senior Officials (Director, Deputy Director [DD], Associate Deputy Director [ADD], and Executive Assistant Directors [EAD]), or their designees:

FBI senior officials or their designees must:

- Identify, compile, and provide all paper records and electronic information systems in which records have been created and stored, which have not otherwise been imported or saved in an approved recordkeeping system, and advise IMD ten days prior to departure of the position, in accordance with section 4.3.7.3.
- Adhere to the policy set forth in DOJ Policy Statement 0801.02 Section I concerning the removal of DOJ information.

2.8. FBIHQ Divisions, Field Offices, and Legal Attaché Offices

2.8.1. ADs, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), and Legal Attachés (LEGAT)

ADs, SACs, ADICs, and LEGATs must:

- Ensure their respective FBIHQ division, FO, or Legat comply with IMD's policies for creating, approving, and maintaining adequate and proper documentation of all official programs and activities, including proper indexing in Sentinel and in other electronic recordkeeping systems.
- Appoint a Records Liaison (RL) via a Sentinel lead to [redacted] to implement records and information management policies and procedures related to hard copy paper records as provided by IMD.
- Ensure the appointment of Information Asset Managers (IAM) for each unit or office within their area of responsibility (AOR) via a Sentinel lead to [redacted] to implement records and information management policies and procedures related to electronic record or nonrecord information stored on all enclaves and in all repositories as provided by IMD. b7E
- Ensure system owners create and maintain data backups for all electronic information systems within their AOR for the requisite time period, in accordance with section 4.2.3.5.
- Appoint an ERO via a Sentinel lead to [redacted] to assist the ERP manager with implementation of the essential records program in accordance with section 4.6. as well as ensure FBIHQ division or FO comply with the ERP and commit adequate resources and training to enable FBI personnel to participate in and complete essential records requirements.

- Respond to periodic FBI records inventories and compliance reviews and complete corrective actions to facilitate the efficient retrieval and sharing of information in support of the FBI's mission.
- Provide resources and time to enable personnel to participate in and complete records and information management requirements and training.
- Establish criteria for self-approval of certain administrative nontransitory records in Sentinel.
- Incorporate approved records and information management questions into the exit checklist to ensure departing FBI personnel have addressed all record and information assets prior to departure or as the result of an organizational change.
- For ADICs/SACs, ensure their respective FO successfully meets the established field office measures as reported through the Integrated Program Management Tool.

2.8.2. Records Liaison (RL)

RLs must:

- Represent their respective FBIHQ division, FO, or Legat by coordinating with IMD on all records and information management policies, procedures, and programs.
- Understand and apply records and information management concepts and federal records management laws and regulations.
- Communicate and direct the application of records management policies and procedures to IAM.
- Oversee the creation and maintenance of records in their respective FBIHQ division, FO, or Legat, and advise FBI personnel of their recordkeeping requirements.
- Provide training on records management policies and procedures, in coordination with IMD's MSS. Coordinate with IMD on the resolution of issues involving FBIHQ division, FO, and Legat files and ensure the inventory error rate is at an acceptable level.
- Maintain an active SCINet account and coordinate with IMD to ensure management of all TS/SCI records and information on the SCINet SharePoint environment, in accordance with section 4.2.2.3.
- Conduct periodic records audits and inventories, in coordination with the ARO.
- Report damage to records promptly to the program manager of ISS' Records Protection and Recovery Program.
- Report missing hard copy case files and serials promptly to ISS and report missing files and serials which contain classified material or PII to their CSO via email, in accordance with section 4.3.9.7.
- Report missing hard copy case files and serials subject to a legal hold promptly to OGC's LTMS, in accordance with section 4.3.9.7.

2.8.3. Information Asset Manager (IAM)

The IAMs must:

- Be knowledgeable of the filing repositories and organizational methods used for all electronic data, information, and records in their respective program, office, unit, or squad.
- In collaboration with the RL, assist and provide guidance to their program, office, unit, or squad, in managing all electronic repositories on all enclaves.
- Develop a file plan and organize their office's hard copy and electronic nontransitory records (regardless of enclave) and annually review and update the file plan as necessary, in accordance with sections 4.3.2. and 4.3.5.
- Provide oversight to ensure periodic reviews are completed (e.g. annually) and to enact disposition of short-term temporary administrative records or guidance to import long-term administrative and investigative nontransitory records to an approved recordkeeping system (e.g. Sentinel), in accordance with sections 4.4.4. and 4.4.5.8.
- Maintain an active SCINet account and coordinate with IMD to ensure management of all TS/SCI records and information on SCINet SharePoint, in accordance with section 4.2.2.3.
- Assist in periodic records audits and inventories, in coordination with the ARO.
- Report missing or destroyed electronic record material which has not met its retention period that is not already stored in an approved electronic recordkeeping system (i.e. Sentinel) to ISS. Promptly report to their CSO via email any missing or destroyed electronic information or records which contain classified material or PII, in accordance with section 4.3.9.7.
- Report missing electronic information or records subject to a legal hold promptly to OGC's LTMS, in accordance with section 4.3.9.7.

2.8.4. System Owners (i.e. Program Managers and Business Owners)

System owners must create and maintain data backups for all electronic information systems, within their AOR for the requisite period of time, to ensure the authenticity, reliability, and integrity of the system's information, in accordance with section 4.2.3.5.

2.8.5. SharePoint site owners, content managers, and content administrators

SharePoint site owners, content managers, and content administrators must submit requests for the creation of SharePoint sites, shared drives, and MS Team sites, and manage site content. They must ensure all records have been entered into an official recordkeeping system relevant to the specific enclave, and submit requests for decommissioning SharePoint sites when no longer needed for business use, in accordance with section 4.2.2.4.

2.8.6. Essential Records Officers (ERO)

ERO must:

- Represent their FBIHQ division or FO by coordinating with the IMD's ARO on all essential records policies, procedures, and programs, ensuring essential records are identified and maintained, in accordance with section 4.6.

- Consult with division or FO ISSO regarding secure storage and protection of electronic essential records.
- On an annual basis:
    - Coordinate with IMD to assess possible threats and risks to records in their FBIHQ division or FO in order to determine level of protection or response required.
    - Prepare and update lists of essential records and methods of protection for FBIHQ division or FO essential records.
    - Draft and submit the ERP and certify it has been reviewed and updated annually. EROs are responsible for creating Essential Records Plans, in addition to their administration and maintenance requirements.
    - Update and upload FBIHQ division or FO Essential Records Plans to the central Essential Records Program SharePoint by the established deadline. EROs may also upload the FBIHQ division or FO Essential Records Plan to their respective SharePoint site.
    - Conduct essential records briefings, training sessions, and validation tests within assigned FBIHQ divisions and FOs.
- Requirements for Legat offices are addressed separately by the Department of State under the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (as amended) which provides COOP and critical infrastructure protection for United States government employees stationed outside of the United States.

2.9. FBI Personnel

FBI personnel must:

- Create and maintain adequate, complete, accurate, and proper records of FBI programs, investigations, activities, decisions, and transactions in accordance with applicable laws and regulations.
- Complete annual records and information management training.
- Serialize all nontransitory records into certified electronic recordkeeping systems, such as Sentinel or successor system.
- Index all nontransitory records filed into Sentinel in accordance with the Indexing User Manual for Sentinel.
- Manage all nonrecord material and transitory records created or stored in various repositories, removable media, personal hard drive, network and shared drives, emails, SMS/texts and electronic instant messages, phone logs, and non-operational SharePoint sites regardless of enclave, and routinely disposition or delete nonrecord and transitory record material when no longer needed for reference or business use, unless an exemption applies or the information is subject to a legal hold, FOIA request or other external request such as discovery or congressional requests. Nonrecord and transitory record material are subject to the *Managing Nonrecord Information and Information Expiration Policy Directive* (1075D)..

- Ensure all records (nontransitory and transitory), nonrecord material, and personal papers, regardless of medium or format, made or received while in the FBI's service have been properly recorded or legally disposed of or transferred to other personnel prior to separation from FBI service, departure from position, or as the result of an organizational change, in accordance with approved retention schedules and *Managing Nonrecord Information and Information Expiration Policy Directive* (1075D).
- Cooperate with FBIHQ division, FO, and Legat RLs and IAMs in the creation, maintenance, and disposition of FBI records and nonrecord material.
- Ensure all deletion, destruction, or removal of FBI records and nonrecord materials comply with federal records management directives, policies, and procedures as well as those policies and procedures established by IMD.
- Notify the RLs and IAMs within their respective office of any missing files or serials immediately upon discovery, in accordance with section 4.3.9.7.
- Comply with legal hold obligations.
- When procuring or operating scanning devices for records purposes, including serializing into Sentinel and other recordkeeping systems, ensure scanning devices are set to the minimum acceptable scanning resolution and optical character recognition (OCR) functions to produce text-searchable images for documents which contain text per section 4.2.3.3.
- Comply with scanning standards set forth in this PG to ensure efficiency and accuracy in the FBI's transition from a hard copy to an electronic-based recordkeeping system, in accordance with section 4.2.3.3.
- When serializing foreign language documents, a translated version must also be serialized. The translated version must be:
    - Certified by the Language Services Section or a machine translation; however, for a machine translation document, the following disclaimer must be documented in the "Document Synopsis" field in Sentinel, "The imported document is a machine translation. Before pursing any law enforcement action or using the enclosed translation in an intelligence assessment, it must be certified by the FBI's Language Services Section."
    - Indexed per the DIOG and the Indexing User Manual for Sentinel.
- Assist EROs with the identification and protection of essential records, and ensure the deletion, destruction, or removal of essential records complies with FBI policies and procedures, in accordance with section 4.6.

3. Policy Statement

IMD establishes the requirements, procedures, and policies necessary to ensure records and information are properly managed in accordance with applicable laws and regulations. All FBIHQ divisions, FOs, and legats are required to incorporate records management laws, policies, and practices, as provided by IMD, into the operation of all FBI programs and investigations to ensure FBI actions, decisions, and operations are appropriately documented and preserved.

All FBI personnel are responsible for identifying, capturing and importing records into the FBI's certified electronic recordkeeping systems; therefore, it is critical to understand the legal requirements, policies, and procedures governing the FBI's records and information management program.

This PG sets forth the policies, requirements, and procedures for managing the FBI's records and information.

4. Processes and Procedures

4.1. Records and Information Management

All FBI personnel must adequately and properly document all information which constitutes a federal record.

A record is all recorded information, regardless of form or characteristic, 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 Government or because of the informational value of data in them. See 44 U.S.C. §3301.

The term '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.

All FBI personnel must upload into the appropriate certified electronic recordkeeping system all information made or received by the FBI which constitutes a federal record (i.e. nontransitory record). A federal record includes both the record content and associated metadata.

4.1.1. Types of Records

FBI personnel must examine information for record status and if deemed a record, determine whether it is nontransitory or transitory (see subsections 4.1.1.1. and 4.1.1.2. for more information). Records can exist in any medium, platform, or technology. Therefore, FBI personnel must examine the content of the information, and not the form, to determine record status.

FBI personnel unable to determine record status must contact the IMD Help Desk for assistance.

4.1.1.1. Nontransitory Records

FBI personnel must preserve all nontransitory records in accordance with records management laws and regulations outlined within this PG. FBI personnel must upload all nontransitory records into a certified electronic recordkeeping system, such as Sentinel. See the *Electronic Recordkeeping Certification Policy Guide* (0800PG) for more information.

A nontransitory record is a record needed for more than 180 days and possesses one or more of the following characteristics:

- contains information necessary to adequately and properly document the activities and functions of the agency;
- provides documentation of agency decisions and commitments reached orally (person-to-person, phone, video, or in conference);
- conveys information of value on agency activities and adds understanding of agency operations and responsibilities;
- documents the formulation and execution of policies and decisions; or
- provides proof of fiscal or legal rights and obligations.

Examples of nontransitory records include, but are not limited to:

- electronic communications (EC);
- FD-302, "Form for Reporting Information That May Become the Subject of Testimony";
- subpoenas;
- search warrants; and
- emails, voicemails, or text and electronic instant messages which contain substantive case information.

FBI personnel should consider the following factors in determining whether information is a nontransitory record. The information is:

- required to be documented by law, regulation, policy, or an established business practice applicable to the FBI;
- pertinent to an FBI investigation (including assessments) or intelligence-gathering activities;
- essential to protect the rights of the government or an individual affected by government action;
- reasonably necessary to document or explain the basis for a significant action or decision involving the exercise of government authority;
- needed to conduct government business effectively;
- maintained to adequately and properly document content within a working file, such as preliminary drafts and rough notes, and the draft was circulated or made available to employees for official purposes such as approval, comment, action, recommendation, follow-up or to communicate with agency staff about agency business, and the draft contains unique information such as substantive annotations or comments which adds to a proper understanding of the agency; or
- necessary to document other significant operations or administrative matters. Examples include: changes in the FBI's organizational structure, changes in FBI-wide or FBIHQ division policies, accomplishment of an FBI mission responsibility, expenditure of funds, a disposition of FBI property, and compliance or noncompliance with a legal obligation.

Whether a document is a copy or original does not determine record status. Several copies of a single document may constitute a record if each copy serves a separate administrative purpose and is maintained in different filing systems. Also, copies of other government agency (OGA) records may constitute a record and require preservation.

4.1.1.2. Transitory Record

FBI personnel must not import transitory records into the FBI's electronic recordkeeping systems. FBI personnel must destroy or delete transitory records when no longer needed for business use, unless subject to a legal hold, FOIA request, or other external request.

A transitory record is a temporary record that is (1) needed for a short time (generally less than 180 days) and (2) is not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Both criteria must be met for the record to be

transitory. A transitory record has no documentary value on its own and is retained only while there is an operational or business need.

Examples of transitory records include, but are not limited to:

- Messages coordinating schedules, appointments, and events.
- SMS/text messages and electronic instant messages and chats which do not contain information needed for longer than 180 days.
- Emails, voicemails, letters, cover memos, and facsimile cover sheets which do not provide evidence of approval concurrence, or decision-making, or include substantive comments.
- Received copies of circulated internal information such as agency instructions, notifications, circulars, newsletters, and email blasts to employees.
- Messages received from agency distribution lists.
- "To-do" or task lists and assignments.

4.1.2. Types of Nonrecord Information

Nonrecord information is information which does not meet the statutory definition of a record. It includes nonrecord material, working files, and personal papers.

4.1.2.1. Nonrecord Material

FBI personnel must not import nonrecord materials into the FBI's electronic recordkeeping systems. FBI personnel must delete all nonrecord material when no longer needed for reference, unless subject to a legal hold, FOIA request, or other external request.

Nonrecord materials are U.S. Government-owned documentary materials excluded from the legal definition of records and includes unofficial copies of documents kept only for convenience or reference, stocks of publications, and library or museum material intended solely for reference or exhibition.

Examples of nonrecord materials include, but are not limited to:

- Publications of processed documents, such as pamphlets, books, manuals, posters, and maps.
- Tickler, follow up, or suspense copies of correspondence, provided they are extra copies of the originals.
- Blank forms and duplicate copies of documents maintained in the same file.
- Extra copies of documents preserved only for convenience or reference.

All FBI personnel must manage and routinely delete nonrecord material in various repositories, network and shared drives, emails, SMS/text and electronic instant messages, phone logs, and nonoperational SharePoint sites regardless of enclave, unless subject to a legal hold, FOIA request, or other external request. See the *Managing Nonrecord Information and Information Expiration Policy Directive* (1075D) for more information.

Nonrecord material may become a nontransitory record if substantive notes or comments are added to the document and, thus, will require preservation within a certified electronic

recordkeeping system. For example, substantive notes added to a draft document or the completion of a blank form converts the document from nonrecord material to a nontransitory record requiring preservation.

4.1.2.2. Working Files

FBI personnel must not import working files into an electronic recordkeeping system and must delete working files when no longer needed for reference, unless subject to a legal hold, FOIA request, or other external request.

Working files are preliminary drafts and other similar materials, regardless of medium, which have not been approved by an FBI official with authority. However, working files with unique information, such as substantive annotations or comments, are records and may require preservation in a certified electronic recordkeeping system.

4.1.2.3. Personal Papers

FBI personnel must not import personal papers into an electronic recordkeeping system and must delete personal papers when no longer needed.

Personal papers are documentary materials belonging to an individual which are not used to conduct official agency business. Personal papers relate solely to an individual's personal and private affairs or are used exclusively for that individual's convenience. They can exist in any format or medium such as SMS/text and electronic instant messages, email, and voicemail.

All FBI personnel must comply with FBI policy regarding the personal use of government property, such as FBI computers, mobile devices, and network drives. See the *FBI Ethics and Integrity Program Policy Guide* (1120PG).

FBI personnel must separate personal papers from records and other nonrecord information. A document which contains both business and personal information constitutes a record and may require preservation. To sanitize a document, FBI personnel should photocopy the document, delete or redact the personal information, and treat the redacted copy as the federal record.

Examples of personal papers include, but are not limited to:

- Materials accumulated by an individual before joining government service which are not used to conduct Government business, such as previous work files and reference files.
- Materials brought into or accumulated in the office, which are not used to conduct agency business and relate 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, literature from professional organizations, manuscripts and draft of articles and books, and an employee's copy of their Standard Form (SF)-50 "Notification of Personnel Action".

FBI personnel who transmit personal information using government-issued devices, such as computers, laptops and mobile phones, are subjecting the information to FOIA, discovery, or other external requests, even though the information is personal in nature and does not meet the statutory definition of a federal record.

4.2. Records Receipt and Creation

Federal records are 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.

4.2.1. Records Receipt

Information and documentation received from non-FBI personnel and organizations that are derived from non-FBI sources may constitute a nontransitory record and may require preservation, depending upon the conditions under which such materials came into agency custody or were used by the agency.

4.2.1.1. Information Received from Non-FBI Personnel and Organizations

FBI personnel must upload to a certified electronic recordkeeping system any information or documentation received from non-FBI personnel or organizations which the FBI must or does take action in the course of its routine duties and responsibilities. The information and documentation are considered nontransitory records, even though it was created by non-FBI personnel or another organization. Examples include information received through the tip line via email and facsimile (fax).

An exception to the above is non-FBI-generated, evidentiary material seized by the FBI or its law enforcement partners or acquired through court order, warrant, federal grand jury or administrative subpoena or voluntarily provided in the course of an investigation of a particular case or intelligence assessment. This evidentiary material, whether physical or in digital form, is treated as evidentiary property and is managed under a different set of rules and regulations than those defined in this PG. Note the FD-1004, "Evidence Chain-of-Custody," is a nontransitory record because it documents the management of evidence. For more information regarding evidence, see the *Field Evidence Management Policy Guide* (1209PG), *Digital Evidence Policy Guide (0830PG)*, and the *Domestic Investigations and Operations Guide* (DIOG).

4.2.1.2. Information Derived from Publicly Available Sources

FBI personnel who obtain information through publicly available sources, such as the internet, which the FBI must or does take action in the course of its routine duties and responsibilities are nontransitory records. FBI personnel must upload the nontransitory records into an ERKC system even though the information was derived from non-FBI sources. For example, a Google map showing the route human traffickers use to move across U.S. borders is not FBI created but is used in furtherance of an investigation. In this instance, information generated from non-FBI sources and used in furtherance of an investigation constitutes a nontransitory record and must be imported into a certified electronic recordkeeping system. See the DIOG section 18.5.1 for more information on publicly available information.

Information derived from publicly available sources which are not used in an investigation or otherwise acted upon, are transitory records or nonrecord material and must be deleted or destroyed when no longer needed for business use or reference. See *Managing Nonrecord Information and Information Expiration Policy* (1075D).

4.2.2. Records Creation

FBI personnel create records to document the policies, decisions, procedures, operations, and activities of the FBI. Such records are nontransitory and must be preserved in a certified electronic recordkeeping system.

4.2.2.1. Records Systems

The FBI uses various databases, electronic information systems, and automated records systems to create and upload records and store case and subject information.

System owners must ensure all electronic information systems undergo a records assessment and ERKC review to ensure records are assigned an appropriate retention and confirm the electronic information system meets federal records requirements.

The ARO leads the records assessment and ERKC process. System owners must contact the ARO to confirm existing electronic information systems within their program areas have undergone a records assessment and ERKC review. See the *Electronic Recordkeeping Certification* (0800PG), which sets forth the recordkeeping policies for managing system content.

FBI personnel should direct specific questions regarding individual systems to the responsible system owner.

A records system is distinct from a system of records. A "records system" is an electronic information system where records are created, stored, and maintained in accordance with the Federal Records Act. In contrast, a "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. This term is specific to the Privacy Act of 1974 and not applicable under the Federal Records Act. For more information on systems of records, please see the *Privacy Policy Guide* (1113PG).

4.2.2.2. Sentinel

Sentinel is a certified electronic information management system which serves as the FBI's central recordkeeping and case management system. Sentinel organizes investigative, intelligence, personnel, and significant administrative records using a case classification system.

Per the DIOG, all FBI personnel must index and serialize all nontransitory records into the appropriate case file in Sentinel.

Sentinel:

- Is used to document actions which must be taken or addressed by FBI personnel through lead assignments. Leads are kept as record information in the associated case file.
- Maintains stub records which document a destroyed serial or record.
- Creates placeholders which link records contained in other approved recordkeeping systems, such as Sentinel Gold or other repositories.

4.2.2.2.1. Indexing

All FBI personnel must comply with the indexing policy per the DIOG, section 3 and Appendix J, and must follow the rules maintained by IMD in the Indexing User Manual to ensure proper indexing is completed for persons, organizations, and events.

For investigative and intelligence matters, FBI personnel must create an "entity" to index all subjects including main, victim, and complainant. During file reviews, supervisory special agents must ensure proper indexing is accomplished per DIOG section 3.5.2.

The ARO audits case information to ensure compliance with indexing requirements.

4.2.2.2.2. Serializing Within a Case File or Subfile

FBI personnel must serialize into Sentinel all documents within the case file which:

- meet the definition of a federal record;
- contain information pertaining to the specific case or administrative file; and
- are not duplicates of records already serialized within the case.

Sentinel automatically assigns sequential serial numbers to each nontransitory record created or imported into the case file which has been approved for serialization.

FBI personnel must serialize any duplicate copies of nontransitory records which contain substantive notes rendering the copy a separate, original record.

4.2.2.2.3. Subfiles

FBI personnel should use subfiles to aid in the organization and administration of substantive case files which have become voluminous or complex. Subfiles are separate files established under the main file which facilitate the efficient retrieval of pertinent information. Subfiles are established on a case-by-case basis and are opened as needed. FBI personnel must obtain supervisory approval prior to opening a new subfile.

IMD is the only division authorized to open new 319 and 67Q case files or subfiles. See section 4.3.4. and the Classifications 319 & 67Q Guide for more information.

4.2.2.2.3.1. Standardized Subfile Names

FBI personnel must follow the guidance in Appendix J of the DIOG to open new subfiles for specifically described investigative or administrative activities. Appendix J contains a list of standardized subfile names.

FBI personnel must use alphanumeric characters such as FF1, FF2, and FF3 to indicate more than one subfile exists for the specific investigative or administrative activity.

4.2.2.2.3.2. Non-Standardized Subfile Names

FBI personnel must create unique subfile names for investigative and administrative activities that are not specifically addressed in DIOG Appendix J. FBI personnel must only use alpha (i.e., A-Z) or numeric (i.e., 0-9) characters, and underscores to create unique main or subfile names, for example, 245B-BA-1234567_SUS. Special characters and symbols must not be used in subfile names.

4.2.2.2.3.3. Classified Subfiles

FBI personnel must not create separate subfiles for classified information within Sentinel. Sentinel is classified at the Secret level. Thus, all Secret, Confidential, and Unclassified serials can be maintained in the same case file. Each serial must be classified at the highest level of classification for the content of the serial (i.e., if the case title is classified, and the title appears in the document, the entire document or serial is classified).

If the case content, contains both classified and unclassified serials, is printed into paper format or copied to electronic data storage media, then FBI personnel must classify all material at the highest classification level. For paper subfiles which contain Secret material, FBI personnel must classify the hard copy subfile at the Secret level. FBI personnel should retain the classification of the main file and all other subfiles, and must not classify it Secret unless it contains Secret material.

4.2.2.2.4. Digital and Physical 1A/1C Packages

FBI personnel must use 1A/1C packages to attach physical and digital documents as well as non-evidentiary, non-chain-of-custody items to the investigative case file.

FBI personnel are prohibited from uploading or retaining evidence or contraband, such as child sexual abuse material (CSAM), in the 1A/1C package, with the exception of material obtained in response to a Grand Jury subpoena return and absent a chain of custody. Please reference the physical and digital requirements outlined in DIOG sections 18.6.5.13.1. and 18.6.5.13.2.

FBI personnel must follow the *Field Evidence Management Policy Guide* (1209PG) and the *Digital Evidence Policy Guide* (0830PG) for guidance regarding the storage and handling of physical and digital evidence, and the *Crimes Against Children and Human Trafficking Program Policy Guide* (1157PG) for the proper handling of CSAM.

4.2.2.2.4.1. Original Hard Copy Documents and Records

FBI personnel must digitize all hard copy documents and nontransitory records and import the digitized document or record into Sentinel as a digital 1A/1C to ensure it is available and searchable to the Bureau. See section 4.4.5.2.2. for information on temporary, nontransitory records.

In some cases, FBI personnel must retain certain investigative nontransitory records in their original hard copy format as required by law or FBI policy. Examples of originals which must be retained include, but are not limited to, handwritten interview notes of FBI personnel, handwritten text, markings, initials, or signatures of third parties, notarized documents, any investigative materials or documents having future evidentiary value, such as Grand Jury subpoena returns absent a chain of custody, or when specifically required by applicable law or policy to be maintained in their original format. Please see the *Importing Nontransitory Records Into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1001D) for more information. Please see DIOG sections 18.6.5.13.1. and 18.6.5.13.2. for the physical and digital storage requirements of material obtained in response to a Grand Jury subpoena return and absent a chain of custody.

In such cases, FBI personnel must use the physical 1A/1C envelope to store and retain original hard copy documents while the case is open. If it is legally determined by OGC or the U.S. Attorney's Office that contents of a 1A/1C may be dispositioned and removed from a case file,

FBI personnel must disposition the item and update the stored location in Sentinel noting the disposition prior to case closure. FBI personnel must inventory physical 1As/1Cs prior to transferring files to the CRC.

Prior to Sentinel, 1A/1C envelopes were received, stapled, or paper-clipped to a document (e.g., an EC or FD-302). FBI personnel would upload and serialize the document, and place the file number and serial number in the lower right corner of the document. FBI personnel would also write the serial number of the document onto the 1A/1C envelope under the "serial number of originating document" line and enter the 1A/1C into the Collected Items Database, which generated a unique 1A/1C number that was placed on both the 1A/1C envelope and document. FBI personnel would file both items into the physical case file.

4.2.2.2.4.2. Electronic and Audiovisual Records

FBI personnel must attach non-evidentiary electronic and audiovisual nontransitory records as a digital 1A/1C to the relevant serial within Sentinel. FBI personnel must remove any passwords and encryption before importing documentary or audiovisual records into Sentinel. FBI personnel must index all subjects within these records.

FBI personnel must store electronic and audiovisual records, which are kept in their original, physical format, within the physical 1A/1C in accordance with the following instructions:

- Mark the electronic and audiovisual record with the appropriate case file number, serial number, or 1A/1C number, if applicable.
- Attach the password to any physical media that was already password protected.
- Create a serial in Sentinel in the relevant case file to document the existence of the physical 1A/1C, including a description of the physical media, any unique playback requirements including passwords and a synopsis of the information in the media, as well as update the volume location in Content Manager (e.g. closed file room, safe, etc.).
- Insert the serial location for the physical 1A/1C in Sentinel under the Actions Tab in the Update Stored Location field and revise as needed.
- Store magnetic media, including open-reel sound recordings and video cassettes away from other electronic devices, magnetic fields, and 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 designated areas protected against unauthorized access and exposure to fire, water, chemicals, insect infestation, vibration, sunlight, and dust.
- 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.

Please see DIOG sections 18.6.5.13.1. and 18.6.5.13.2. for the digital and physical storage requirements of material obtained in response to Grand Jury subpoena returns and absent a chain of custody.

4.2.2.2.5. Encrypted and Password Protected Serials and 1A/1C Attachments

FBI personnel are prohibited from encrypting or password protecting any digital content imported or attached as a digital 1A/1C. Encrypted or password protected digital content will not populate during an automated Sentinel search, which could cause FBI personnel to miss critical investigative information and potentially jeopardize national security.

In addition, IMD cannot access or delete encrypted or password protected serials in response to permanent charge out (PCO) requests. FBI personnel needing to control access should consider restricting files in Sentinel. See the *Manual Restriction of Access to Data in FBI Case Files Policy Notice* (0758N) for more information.

4.2.2.2.6. Foreign Language Documents

FBI personnel must obtain a machine translation of all foreign language documents that are digitally born and where a certified translation is not already available. FBI personnel must serialize the English translation as a digital 1A into Sentinel. FBI personnel must also index the document per the DIOG and Indexing User Manual. FBI personnel must ensure that the English translation is either certified by the Directorate of Intelligence's Language Services Section (LSS) or the result of a machine translation prior to serializing into Sentinel. Contact the LSS for questions regarding authorized machine translation programs.

For a machine translation, FBI personnel must include the following disclaimer within the "Document Synopsis" field in Sentinel: "The imported document is a machine translation. Before pursuing any law enforcement action or using the enclosed translation in an intelligence assessment, it must be certified by the FBI's Language Services Section."

4.2.2.3. TOP SECRET (TS) Information and/or Sensitive Compartmented Information (SCI)

FBI personnel must manage digital-born TS or SCI nontransitory records within the respective SCINet recordkeeping system, i.e. SharePoint environment or Sentinel Gold.

The RLs and IAMs, as appropriate, must have an active SCINet account and must oversee the management of all TS/SCI records and information on SCINet. See section 4.2.2.4. for requirements on the creation, maintenance, and decommissioning of SharePoint sites.

FBI personnel who create or receive digital-born TS or SCI nontransitory records must upload, manage, and store records within the appropriate SCINet recordkeeping system. In FBINet Sentinel, FBI personnel must serialize a record to document the existence of the digital or physical TS or SCI nontransitory record (and FISA material at the TS or SCI level). Once the record has been serialized in Sentinel, FBI personnel must maintain the TS or SCI material either in the SCINet SharePoint environment, Sentinel Gold, or within the Sensitive Compartmented Information Facility (SCIF) in accordance with TS or SCI storage and maintenance polices.

For guidance on the serialization of TS or SCI material, please see the IMD One-Shot – Digital TS-SCI Material and the IMD One-Shot – Non-Digital TS-SCI Material.

4.2.2.4. SharePoint Sites

FBI personnel must create, maintain, and decommission all SharePoint sites regardless of enclave – SCINet, FBINet, and UNet - in accordance with governing laws, regulations, and policies relevant to records management, privacy, and electronic discovery (e-Discovery).

The RL or IAM must assign site owners, content managers, and content administrators for each FBIHQ division, FO, and Legat operating a SharePoint site.

Site owners, content managers, and content administrators must:

- Submit completed SharePoint site creation requests located on ITADD's Web Services Unit (WSU) intranet site and agree to all provisions on the request.
- Manage information and records housed on SharePoint sites under their cognizance in accordance with applicable laws, regulations, policies, and guidelines, including those for specific enclaves or specific SharePoint instances.
    - Ensure nontransitory investigative records are exported to the appropriate ERKC system.
    - Manage nontransitory administrative records on SharePoint for the entire lifecycle of the record and disposition or delete based on applicable retention schedules absent a legal hold, FOIA request, or other external request.
    - Delete any transitory records or nonrecord information that is no longer needed for business use or reference and is not subject to a legal hold, FOIA request, or other external request.
- Provide oversight and ensure compliance with relevant authorities and policies.
- Ensure users are granted access to sites and have notice of compliance requirements.
- Complete SharePoint site decommissioning requests located on ITADD's WSU intranet site and agree to all provisions of requests prior to routing requests to IMD and OGC for final decommission approval.
- Coordinate with both OGC and IMD and review all electronic information content, including SharePoint discussions, tasks, calendars, or lists for records and/or information subject to legal holds, prior to site decommissioning.

RL or IAM must:

- Assign site owners, content managers, or content administrators, as appropriate, to operate SharePoint sites for respective FBIHQ division, FO, or Legat.
- Maintain an active SCINet account and oversee the management of all TS/SCI records and information on SCINet SharePoint.

The IMD must:

- Advise FBI SharePoint users, site owners, content managers, or content administrators regarding SharePoint content management and records and information management responsibilities.
- Process SCINet SharePoint site requests within ten business days.

- Conduct decommissioning reviews of site on all enclaves as referenced on SharePoint site decommissioning requests, within 20 business days of receiving requests, to confirm or deny eligibility.
- Review the SCINet SharePoint request and provide approval or denial of SharePoint site decommissioning requests to ITADD staff.

OGC's LTMS must:

- Provide guidance to FBI SharePoint users, site owners, content managers, and content administrators regarding SharePoint content, privacy, and e-Discovery responsibilities.
- Conduct decommissioning reviews of sites referenced on SharePoint site decommissioning requests, within 20 business days of receiving the request, to confirm or deny eligibility.
- Review request and provide approval or denial of SharePoint site decommissioning requests to ITADD staff.
- Consult with OGC's PCLU, as appropriate, on privacy-related matters.

After the IMD's and LTMS's reviews, ITADD must approve or deny SharePoint site creation or decommissioning requests and notify site requestors.

ITADD must:

- Create SharePoint sites within ten business days of approving the request and grant site access for review purposes to designated IMD and OGC personnel.
- Complete decommissioning of SharePoint sites within ten business days of approving the SharePoint site decommissioning request.
- Ensure the decommissioning request contains a verification statement from the requester stating that all nontransitory records were uploaded to an ERKC system prior to submitting the request.
- Notify the Executive Writing and Organizational Communications Unit in the Office of Public Affairs (OPA) if the site is an FBI intranet presence site.
- Manage information and records submitted for creating and decommissioning the site, in accordance with applicable laws, regulations, policies, and guidelines.
- Maintain decommissioned SharePoint sites on backup tape in accordance with section 4.2.3.5. of this policy guide.

4.2.3. Electronic Records

4.2.3.1. Email and Other Electronic Messaging Tools

Electronic messaging tools are technologies used to facilitate the exchange of information and to allow FBI personnel to share, discuss, and collaborate on information, ideas, projects, and activities. Electronic messaging tools encompass both (1) point-to-point communication tools such as emails, instant and text messaging, digital and wireless phone calls, voicemail, Voice over Internet Protocol (VoIP), online and audio meeting and conferencing, and (2) web-based tools such as shared mail services (e.g. shared calendars), video and photo-sharing sites, virtual

bulletin boards, wikis, blogs, and professional- and social-networking sites. The guidance in this section applies to all FBI information transmitted through both U.S. Government issued devices and nonofficial or personal devices.

FBI personnel must identify, capture, and upload to a certified electronic recordkeeping system all electronic messages which constitute a nontransitory record. An electronic message may be nontransitory, transitory, or nonrecord depending on the content of the communication but not the form. Information transmitted through electronic messaging tools are generally transitory records or nonrecord material and can be deleted when no longer needed for reference absent a legal hold, FOIA request, or other external request. When doubt exists about the record status, FBI personnel must contact the IMD Help Desk.

FBI personnel must import electronic messages in the format in which they were generated, otherwise known as the "native format," if uploading capabilities exist for the particular ERK system. If an electronic message cannot be imported in its native format, such as a voicemail message, then FBI personnel must memorialize the nontransitory record content in another format (e.g. FD-302 or EC) with the relevant metadata and upload into the appropriate certified ERK system within 20 days after the original creation or transmission date. See section 4.2.3.4. for metadata requirements.

FBI personnel should not create or send records (transitory or nontransitory) using personal devices or through nonofficial electronic messaging accounts. However, FBI personnel who transmit or receive a record through a personal device or nonofficial account must (1) copy their official FBI electronic messaging account in the original creation or transmission of the record, or (2) forward a complete copy of the record to their official electronic messaging account no later than 20 days after the original creation or transmission of the record. Once received in their official electronic messaging account, FBI personnel must immediately import or upload the nontransitory record into a certified ERK system.

Electronic messages transmitted in connection with federal criminal cases have special preservation requirements. See the *Preservation and Disclosure of Electronic Communications in Federal Criminal Cases* (0423D).

Electronic messages sent by senior officials have special handling requirements. Point-to-point communications, such as instant and text messages, from senior officials and sent externally to the public are nontransitory records and must be captured in a certified ERK system with the relevant metadata. Senior officials may send instant and text messages internally or to other federal agencies, state, local, and tribal governments which contain information related to decisions or actions. If this information has not been otherwise memorialized and captured in a recordkeeping system, the senior official must import the message into a certified ERK system with the relevant metadata.

4.2.3.1.1. Email

Emails may be nontransitory, transitory, or nonrecord. FBI email systems are not recordkeeping systems; therefore, FBI personnel must import all nontransitory record emails into a certified ERK system. When doubt exists about the record status, it should be treated as a nontransitory record email and preserved within 20 days after the original creation or transmission date.

FBI personnel must delete all transitory and nonrecord emails that are no longer needed for business use or reference, absent a legal hold, FOIA request, or other external request. See the

Managing Nonrecord Information and Information Expiration Policy (1075D) and *Legal Hold Policy Directive* (0619D) for more information.

4.2.3.1.1.1. Nontransitory Record Emails Sent via SCINet, FBINet, and UNet

SCINet

- On SCINet, FBI personnel must move nontransitory record emails into SCINet Sentinel Gold, which is the approved recordkeeping system for SCINet. FBI personnel must also create a placeholder serial in Sentinel tagged with the appropriate case classification which references the nontransitory record email.

FBINet

- On FBINet, FBI personnel must use the Record Marking Tool (RMT) in Microsoft Outlook to tag emails as nonrecord, transitory record, or nontransitory record and select the appropriate case file number. The RMT uploads the nontransitory record email into the Sentinel workflow, which is then serialized into the case file.

UNet

- On UNet, FBI personnel send and receive emails from various accounts on the unclassified enclave such as LEO email, fbi.gov account, ICE mail, or SIPRNet. FBI personnel must import into Sentinel all nontransitory record emails sent or received using UNet. FBI personnel must utilize "Uplift" to bring the email to FBINet and then send the email to their FBINet account using the RMT tool to tag the email as nontransitory. The RMT uploads the nontransitory record email into the Sentinel workflow which is then serialized into the case file.

Electronic recordkeeping systems without an automated upload option [redacted] must be captured manually. FBI personnel must memorialize the record content with the relevant metadata into an EC or FD-302 and upload it into the appropriate certified ERK system. See section 4.2.3.4. for more information on metadata. As part of the record, FBI personnel must also save and upload all email attachments. b7E

Nontransitory record emails must be uploaded to the appropriate case file(s) in Sentinel or into the appropriate ERKC system prior to deleting the original online email.

4.2.3.1.1.2. Transitory Record and Nonrecord Emails

FBI personnel must delete transitory record and nonrecord emails which are no longer needed for business use or reference, unless subject to a legal hold, FOIA request, or other external request. FBI personnel should not comingle record and nonrecord information within emails to ensure nonrecord information is not inadvertently transferred and retained in one of the FBI's electronic recordkeeping systems. A document which contains both business and nonrecord information constitutes a record and requires preservation.

4.2.3.2. Other Electronic Messaging Tools

Other electronic messaging tools include point-to-point communication tools such as text and electronic instant messaging, digital and wireless phone calls, voicemail, Voice over Internet Protocol (VoIP), online and audio meeting and conferencing, as well as web-based tools such as shared mail services (e.g. shared calendars), video and photo-sharing sites, virtual bulletin

boards, wikis, blogs, and professional- and social-networking sites. The guidance in this section applies to all FBI information transmitted through U.S. Government issued devices and nonofficial or personal devices. See section 4.2.3.1. for additional information.

FBI personnel must identify, capture, and upload into a certified ERK system all nontransitory record content transmitted through electronic messaging tools. Communications using electronic messaging tools may be records depending on the content of the communication.

Text Messages

- For text messages on FBI devices, FBI personnel must use Textport, or a successor application, to capture and upload record content into a certified ERK system. Textport is a text message archival application used to retrieve message logs through multimedia applications and to export text messages which contain nontransitory record content into a certified ERK system. See IMD One-Shot – Capturing and Uplifting Text Message Records to Sentinel for more information.
- For text messages on nonofficial devices, FBI personnel must copy and paste the text message into an email and forward it to their official FBI email account no later than 20 days after the original creation or transmission. FBI personnel must immediately import or upload the nontransitory record into a certified ERK system.

Instant Messages

- For FBINet, FBI personnel must preserve all instant messages sent via Skype, or through successor software, which contain nontransitory record content. FBI personnel must save messages in the conversation history folder in Outlook. From there, FBI personnel must move the message from Outlook to Sentinel by sending the message to themselves as an email and using the RMT to mark it a nontransitory record. This process allows FBI personnel to upload instant messages into Sentinel.
- For UNet, FBI personnel must preserve all instant messages sent via Microsoft Teams, or through successor software, which contain nontransitory record content. FBI personnel must save the instant message and uplift to FBINet. From there, FBI personnel must email the message to themselves using the RMT to mark it a nontransitory record. This process allows FBI personnel to upload instant messages into the relevant case file in Sentinel.

Voicemail, online meetings, and other electronic messaging tools

- FBI personnel must manually capture and import into the appropriate electronic recordkeeping system all electronic messaging tools that do not offer automatic upload options (e.g. voicemail, online meetings such as MS Teams, etc.). For Sentinel, FBI personnel must memorialize all record content in an FD-302 or EC with the relevant metadata (e.g. author, date created, date modified, file size) and import it into Sentinel. For other certified ERK systems, FBI personnel must memorialize the record content in an acceptable format for the designated system, as well as capture the relevant metadata (e.g. author, date created, date modified, file size) and import into a certified ERK system. See section 4.2.3.4. for information on metadata requirements.

4.2.3.3. Digitizing Nontransitory Records and Scanning Standards

4.2.3.3.1. Scanner Equipment Standards (including Document Conversion Laboratory Service Requirements)

ISS' DocLab is the FBI's centralized entity for mid- to high-volume scanning and document conversion, including special investigations and major cases throughout the FBI. To obtain scanning support, FBI personnel must submit scanning requests to ISS's DocLab and provide the following information: background, type of material to be scanned, approximate number of boxes or volumes, and desired date for project completion.

ISS' DocLab must scan documents in accordance with the electronic archival standards imposed by NARA and outlined here and in section 4.2.3.3.2. Please see ISS' DocLab SharePoint site for more information on requesting scanning support.

ISS' DocLab will work with FBI personnel to determine the best and most efficient method for scanning and converting documents into electronic format for records which cannot be physically sent to ISS' DocLab for processing.

For small scanning projects, FBI personnel must use FBI-approved desktop scanners up to 75 pages per minute (PPM) or multi-function printers (MFP)/scanners and must ensure scanning output meets the standards set forth in this section and in the following documents: Requirements for Scanned Images of Textual Records and Requirements for Image Formats Converted to Portable Document Format (PDF). When scanning with an MFP, FBI personnel must ensure the configuration settings enable efficient indexing for importing into Sentinel. For example, when using a Lexmark x654de scanner for serializing into Sentinel, FBI personnel must use the following settings: Scan to email, .pdf (searchable), 300 dpi. FBI personnel should contact the IMD Help Desk with questions regarding scanning standards and to confirm scanners meet federal recordkeeping requirements.

4.2.3.3.2. Imaged Records and Standards for Scanned Documents

All FBI personnel must comply with the minimum standards and requirements set forth by NARA and established below when scanning hard copy textual and nontextual records, and converting hard copy records into digital images.

FBI personnel may convert images into searchable files through the use of OCR software resulting in full text searchable files. The decision to convert records into images or to OCR is based on an office's business needs balanced against the costs.

All FBI personnel must obtain authorization from ISS' DocLab prior to converting records created in one particular media or file format into another.

FBI personnel may request a change in media format for several reasons:

- there is a legal requirement (e.g., NARA transfer, evidence in court);
- current format is obsolete;
- non-standard or no longer supported by the manufacturer or FBI recordkeeping systems; or
- another format better meets the business needs.

FBI personnel must comply with minimum requirements when scanning and converting hard copy textual and nontextual documents into digital images. Please see ISS' DocLab SharePoint site for scanning and converting requirements and reference the following documents: Requirements for Scanned Images of Textual Records and Requirements for Image Formats Converted to Portable Document Format (PDF). See section 4.2.3.3.3. for information on nontextual records such as maps and photographs.

FBI personnel, who procure or operate scanning devices for records purposes, including serializing into Sentinel or other recordkeeping systems, must ensure the scanning devices operate in the correct settings and the OCR function is set to produce text-searchable images for documents which contain text. FBI personnel should contact ITB to ensure scanners are operating in accordance with these standards. ISS periodically updates the list of acceptable scanning formats and versions on its intranet page.

ISS' DocLab also provides scanning services for FBIHQ divisions, FOs, and Legats needing to convert evidence into digital format. FBI personnel must contact ISS' DocLab to obtain evidence scanning services. ISS' DocLab scans evidence onto CDs, DVDs, etc. and does not incorporate digital evidence into 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 CDs, DVDs, etc., is returned to the contributor or destroyed in accordance with the *Field Evidence Management Policy Guide* (1209PG).

4.2.3.3.3. Standards for Photographic Records

FBI personnel must consult with ISS for guidance on converting original photographs or negatives to digital format. FBI personnel must upload the digital conversions into the related investigative case file and retain all digital and negatives generated by the FBI, such as crime scene photographs, since they are nontransitory records and require preservation in a certified ERK system. The photographs will assume the retention period of the related investigative case file.

4.2.3.4. Metadata Requirements

Metadata provides administrative, descriptive, and technical information, which describe the structure and content of electronic records, as well as contextual information about how a record was created, used, managed, and maintained. For example, metadata includes the author, date created, date modified, and file size. The metadata must be detailed and descriptive to effectively manage electronic records throughout their life cycle.

Metadata requirements are needed for effective management of both records and nonrecord information. For recordkeeping purposes, metadata requirements are jointly established by both the originating program office and IMD. With adequate metadata, records and information are retrieved efficiently and disposed when no longer needed. The policy for incorporating metadata tags into electronically stored information is located in the *Electronic Recordkeeping Certification Policy Guide* (0800PG).

4.2.3.5. Data Backup Creation and Retention

All system owners with oversight authority over information technology equipment and processes must create data backups for all electronic information systems within their AOR to ensure the authenticity, reliability, and integrity of the system's information. System owners must retain a full data backup for each FBI electronic information system within their AOR until

superseded by a second subsequent backup that is verified as successful or when no longer needed for system restoration, whichever is later.

For FBINet File/Print Servers, system owners must retain a full data backup for 90 days.

The only exception to the policy are litigation holds, external requests, or other special inquiries whereby system owners must retain full data backups of the electronic information system until OGC's LTMS rescinds the legal hold or preservation request.

LTMS must notify system owners when there is a need to retain the electronic information beyond the standard retention period for a given electronic information system (e.g. Sentinel). LTMS must also notify system owners when an exception to the approved retention period has expired.

4.3. Records Maintenance and Use

FBI personnel must create and maintain authentic, reliable, searchable, retrievable records and ensure they remain so for the length of their approved retention period. The following subsections address the maintenance and use of nontransitory records.

4.3.1. Records Series and Filing Locations

FBI personnel must file nontransitory records into the appropriate record series and filing location. Records are filed according to content and use, regardless of medium, and are divided into record groups (or series) of files. For example, investigative records are filed in the appropriate file classification in Sentinel.

The majority of the FBI's mission-related records are arranged in case files in specific file classifications. FBI file classifications correspond to federal violations over which the FBI has investigative jurisdiction. File classifications are also assigned to intelligence, personnel, and administrative matters.

In contrast, administrative records facilitate routine organizational or "housekeeping" activities. Examples of administrative records include time and attendance, travel vouchers, purchase orders, and budget preparation documents.

4.3.2. File Plan

All offices, through their designated IAM, must develop a file plan to organize their office's hard copy and electronic nontransitory records (regardless of enclave) and should post the file plan as the first file of each shared drive, SharePoint site, or records storage location. File plans are generally based on the topic (record series) and the required retention period. The file plan is a directory of an office's or program's records and includes those records received or otherwise acquired and used in the course of business. It outlines the main file headings and subdivision headings for each record series and information system within an office. It identifies nontransitory records in all media, including paper, electronic, and audiovisual, which are physically stored in the office; electronic records, whether on a local or remote computer server or on removable media; records on other nonpaper media, such as digital video discs (DVD), audiotapes, and film; and records stored in other office file storage areas.

For electronic records, the file plan lists the folders in the shared drive, non-operational SharePoint site, or other repository as well as the calendar or fiscal year associated with the creation of each folder. The FBI's file classification system must be used for folder names. For

administrative records (such as weekly reports), 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, a new folder can be opened for the current year. The 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.

The IAM must annually review the file plan and update as necessary moving inactive and noncurrent files, such as records from the previous year, out of the office's file plan and into another appropriate storage location for the remainder of the retention period. For example, Sentinel has an automated records management application which contains a system file plan. Offices who experience an organizational or structural change should contact the IMD Help Desk for assistance with migrating electronic information and establishing new file plans.

4.3.3. Case File Classification and File Types

FBI personnel must use the appropriate case file classification number when serializing nontransitory records into Sentinel. The majority of the FBI's operational, mission-related records are arranged in case files according to the specific type of investigation or intelligence. When a new case in Sentinel is opened, the user must identify the appropriate case file classification indicating the type of investigation. The office of origin defaults to the user's profile and a file number is automatically created by Sentinel. An example of a file number is 91A-BA-1234576. A complete list of case classifications is maintained on the FBI's Resource Planning Office website.

There are several types of investigative and non-investigative files addressed in the following subsections. Investigative files include assessments, preliminary investigations, full investigations, full enterprise investigations, positive foreign intelligence full investigations, spin off investigations, and unaddressed work. Non-investigative files include control, zero, double zero, and administrative files. See DIOG Appendix J for detailed guidance regarding the management of these file types.

4.3.3.1. Control "C" Files

Control files are established for the purpose of managing programs. Control files must only be used for documenting program management functions and communications, technical or expert assistance to another law enforcement or intelligence agency, or other managerial functions. Control files are designated with the letter "C" before the case number, e.g. 29B-NF-C4456. All entity records in a control file are indexed as references. Control files are, in most instances, nontransitory records with a permanent retention.

4.3.3.2. Zero "0" Files

Zero files contain complaints not initiated as assessments or predicated investigations, or other documents that do not require an investigation (e.g. Information Only leads). Each FBIHQ division, FO, or Legat may open a zero file for each new classification, with the exception of the 319 and 67 classifications. Zero files should be opened only when an office has miscellaneous documents which do not rise to the level of opening a case file. They are opened under main classifications [redacted] and not classifications with designated alphas (e.g., [redacted] Each main case classification should have only one zero file per Office of Origin (OO). The case title must not be indexed and all subjects added to the zero file must be

b3
b7E

indexed as references. Zero files are not opened automatically in Sentinel; rather, FBI personnel must manually open zero files in Sentinel.

If an investigative or administrative case is later opened or identified, FBI personnel must transfer the serialized record from the zero file to the relevant case file. See IMD One-Shot.

4.3.3.3. Double Zero "00" Files

Double zero files may contain documentation, such as instructions, statutes, and decisions, applicable to the classification which do not require investigation.

4.3.3.4. Administrative "A" Files

Administrative files may be opened in all file classifications for administrative purposes only to document non-investigative matters, such as training matters, personnel files, etc.

4.3.4. Management of Classification 319 and 67Q Files

FBI personnel must use classifications 319 and 67Q to file and manage nontransitory administrative and personnel-related records. A subfile exists for each FBIHQ division, FO and Legat for each category of the 319 and 67Q record series.

IMD is the only division authorized to open new 319 and 67Q files in Sentinel. FBI personnel must contact and obtain approval from IMD's ARO to open any new 319 or 67Q case file numbers not already listed in the Classifications 319 & 67Q Guide.

4.3.4.1. Main and Subfiles

FBI personnel must file all nontransitory records of FBI-wide interest or significance into the appropriate 319 or 67Q main file.

FBI personnel must use their respective office's designated subfile to file all nontransitory records which are not widely disseminated (i.e. FBI-wide or to all field offices) or do not have significance beyond their individual office. For example, all budget correspondence created by IMD will be filed in the subfile for IMD's budget matters [redacted] b7E regardless of which section created the record.

Also, FBI personnel must file responses to FBI-wide ECs using their office's designated subfile and must not file it in the FBIHQ main file. Examples:

- Finance and Facilities Division (FFD) issues a Bureau-wide EC from the FBIHQ main file. The Baltimore Field Office (BA FO) must respond to the EC using their office's designated subfile and reference the FBIHQ main file and serial number to which it is responding.
- FFD sends an EC to BA FO only. In this instance, FFD should file its communication in the FFD subfile. The BA FO must respond to the EC using the BA FO subfile and reference FFD's subfile and serial number.

4.3.4.2. Supervisory Approval of Administrative Records in Sentinel

All FBIHQ divisions, FOs, and Legats must establish procedures clearly defining which administrative nontransitory records require supervisory approval prior to importing and serializing into an administrative case file in Sentinel. FBIHQ divisions, FOs, and Legats must establish clearly defined procedures for obtaining required signatures without impeding the

timely serialization of records into the administrative case file and FBI personnel must obtain supervisory approval prior to serializing division-level nontransitory records into an administrative case file in Sentinel. Supervisory approval is not required for importing and serializing administrative records unless specifically designated.

The only exception is nontransitory records imported through Sentinel's workflow by FBI personnel who do not have supervisory functionality. In those instances, FBI personnel should designate themself as the approver when adding administrative nontransitory records and should do so if the particular FBIHQ division, FO, and Legat has authorized self-approval. The approval authority required for investigative records is addressed in the DIOG under section 3.5.2.3.

Supervisors must ensure FBI personnel receive training to ensure documentation requirements are followed. FBI personnel must obtain supervisory approval of division documents which require such approval and for obtaining the approval prior to importing or serializing records into the administrative case file.

4.3.5. Short-Term Temporary Administrative Records

4.3.5.1. Electronic Administrative Records

For electronic administrative records, FBI personnel may use FBINet shared drives or non-operational SharePoint sites to file and manage short-term administrative records (including case file classification 319), which have a retention period of 10 years or less. Shared drives and non-operational SharePoint sites, with the exception of SCINet SharePoint, are not certified electronic recordkeeping systems; however, FBI personnel are permitted to use these repositories for filing and storing short-term temporary administrative records only.

The IAM must organize and manage the file plan within their respective office by adding or deleting folders, assigning security, monitoring use, and assisting with disposition. See section 4.3.2. for information on file plans.

The IAM must annually review records on their office's shared drives and SharePoint sites, and must delete any short-term administrative records which have met their retention. See section 4.3.2. for information on file plans and contact the IMD Help Desk with questions regarding retention or disposition.

4.3.5.2. Hard Copy Administrative Records

For hard copy administrative records, FBI personnel must keep administrative files separate from hard copy investigative or intelligence files. FBI personnel must place hard copy administrative files into a file drawer or cabinet.

FBI personnel must designate and mark each file container (file front and back, drop folder, accordion folder) with the classification number and alpha character, case file number, title of the 67Q or 319 category as it appears in the classification guide, and calendar or fiscal year in which the files were created or received. FBI personnel must avoid unnecessary duplication of records (i.e. do not print records from Sentinel).

4.3.6. Personnel Records

4.3.6.1. Electronic Official Personnel Folder (eOPF)

The FBI's official personnel folder (OPF) is a group of nontransitory records documenting an individual's FBI employment history with the federal government. In March 2013, OPFs were

converted to electronic official personnel folders (eOPF) and are available online for FBI employee access via the eOPF application.

FBI personnel may print and save copies of their e-OPF at any time during employment. FBI personnel may also request copies of their medical information from the FBI Medical Operations and Readiness Unit or other FBI medical personnel. Current and former FBI personnel may request a copy of their FBI paper personnel records by submitting a Privacy Act (PA) request to RIDS. FBI personnel should contact the Human Resources Division's Call Center for questions regarding eOPF.

In addition to the eOPF, the FBI maintains legacy classification 67 hard copy files including security (S) and medical (M) subfiles.

4.3.6.2. Performance Appraisals

In 2018, the FBI transitioned from a paper based to an electronic performance appraisal system. performance appraisals (i.e., Wrap-Ups) have been created and maintained electronically in the HR Source application. Offices with legacy hard copy performance appraisal reports (PAR) in their possession must contact ISS for disposition guidance.

4.3.7. FBI Senior Official Records

4.3.7.1. Director Briefings and Presentations

FBI personnel must serialize into the appropriate administrative or investigate case file all finalized briefings, white papers, reports, and other presentations provided to the Director. FBI personnel must create a Sentinel entity for each presentation or subject to enhance retrievability. It is important to note the subject matter and filing location of the briefing, presentation, white paper, etc. may render the record permanent with eventual transfer to NARA.

4.3.7.2. Records by the Executive Secretariat

The Executive Secretariat (Exec Sec) receives, reviews, and disseminates correspondence from the White House, Congress, Department of Justice (DOJ), and other government entities. Executive level correspondence includes communications 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 managed by the Exec Sec and are maintained in Sentinel under a designated case file. Paper copies must be destroyed as nonrecord material when no longer needed.

4.3.7.3. Records Preservation Requirements for FBI Senior Official Records (Executive Assistant Director [EAD] and Above)

Senior officials are those individuals within an organization responsible for the agency and program policy- and mission-related actions. The FBI's senior officials include the director, deputy director, associate deputy director, and executive assistant directors. NARA has appraised senior official's information as permanent records under disposition authority N1-065-07-001.

Senior official records consist of, but are not limited to, emails, personal notes, annotated briefings not maintained elsewhere, and other documentation received or generated by senior officials in the normal course of business. Examples include: briefings conducted by the senior

official, administrative matters, policy matters, and/or investigative matters, calendars, appointment books, schedule logs, diaries, and other records documenting meetings, appointments, telephone calls, voicemails, trips, visits, and other activities which contain substantive information relating to official activities and have not been incorporated into official files. To the greatest extent possible, senior officials must incorporate these records into the FBI's official recordkeeping system.

Within 180 days of vacating the position, an FBI senior official's records must be transferred to IMD for maintenance and disposition. This policy applies to all FBI senior official's records, regardless of format and across all enclaves.

Prior to departing, all FBI senior officials or their designees must:

- Identify all paper records and electronic information systems in which records have been created and stored, and advise IMD's ISS at least 10 days prior to departure through the following email address: [redacted] on FBINet. b7E
- Adhere to the policy set forth in DOJ Policy Statement 0801.02 Section I concerning the removal of DOJ and FBI information.

ISS must work with ITB to ensure senior official's electronic records are identified upon appointment and collected upon departure from the position.

ITB must collect senior official records from electronic repositories across all enclaves, as well as any successor repositories.

ITB must collect senior official records from UNet's 324Mail, as well as any successor system.

ITB must transfer or maintain the collected records in an agreed-upon format, as directed by IMD.

ISS must:

- Work with ITB to ensure electronic records are collected and preserved in an acceptable format.
- Store and maintain collected hard copy records and electronic media, if appropriate, until disposition.

All FBI personnel requesting access to a senior official's collection must first receive OGC approval.

This policy excludes records managed by the Exec Sec and the Director's Briefing Books.

4.3.8. File Request System (FRS)

FBI personnel must use the FRS to request digital copies of closed hard copy case files stored at the CRC. The FRS replaced the File Request Automation Project (FRAP) and uses an Automated Storage & Retrieval System (ASRS) to store, retrieve, and manage hard copy records.

In response to FRS requests, ISS will provide a digital version of the case file and will no longer furnish the physical file, except in very limited circumstances.

4.3.8.1. Maintaining Custody of Hard Copy Case Files

In limited circumstances when a hard copy case file is provided in response to an FRS request, FBI personnel must maintain physical custody of the case file until it is returned to the CRC to ensure proper security and access control. FBI personnel must not give or lend case files to other FBI personnel. To change custody, FBI personnel must return the case file to the CRC and FBI personnel seeking the hard copy case file must submit a new FRS request. If needed, a convenience copy may be made of the file and must be destroyed when no longer needed for business use, not to exceed the retention date of the closed case file.

4.3.8.2. Returning Case Files

FBI personnel must return all hard copy case files to the CRC within 180 days of receipt. If an extension is needed, FBI personnel must request an extension through the FRS. FBI personnel must attach the FRS request form to the physical case file when returning it to the CRC.

4.3.9. Case File Management

4.3.9.1. Case File Consolidation

FBI personnel must request a case file consolidation in order to move contents from one case file into another. For information on case consolidations, please see the IMD One-Shot.

Pre-Sentinel paper files were consolidated by writing "Consolidated into _____ (new file number)" on the front of the eliminated file and retaining the empty file jacket cover in the closed files section. The notation will appear on older case files.

4.3.9.2. File Transfers

FBI personnel must request a change case request (CCR) in order to transfer cases in Sentinel to other FBIHQ divisions, FOs, and Legats. A CCR must be used to request changes to the owning office, owning squad, case managers, and case participants.

For legacy files, FBI personnel must use case consolidations to transfer legacy files since a CCR could create a duplicate file in the receiving office. For information on CCRs, please contact the IMD Help Desk.

4.3.9.3. Serial Transfers

FBI personnel must request a serial transfer to move serials from one case file into another within Sentinel. A serial stub record is created and added to the original case file in place of the transferred serial. The stub record serves as a placeholder to document the removal of a serial and assumes the original serial number of the case file. The stub record lists the case to which the serial was transferred, why, when, and by whom. IMD does not have the ability to further transfer a serial once it has been transferred into the correct case file. For additional guidance, please see the IMD One-Shot.

4.3.9.4. Case Status

FBI personnel must request a CCR to change the status of a case file within Sentinel. The DIOG addresses the closing standards, approvals, and notice requirements for investigations. It also addresses the process for placing cases in a pending inactive status.

For hard copy case files that close, FBI personnel must mark a line through the assigned special agent (SA) or squad name on the file jacket cover and must write a "C" on the line above, as well

as the date the file was closed in the case management system. FBI personnel must use the following notations: (1) C4 for administrative closing, (2) C5 for United States Attorney declination, or (3) C6 for other. When a case is placed in pending inactive status, FBI personnel must mark a line through the assigned SA or squad name and on the line above write a "P" and the date to indicate it is pending inactive.

4.3.9.5. Deletion of a Record (Permanent Charge Out)

FBI personnel are prohibited from deleting or destroying nontransitory records without specific authorization from IMD. IMD is the sole entity with authority to destroy or delete, or authorize others to destroy or delete, nontransitory records, in accordance with applicable laws and NARA-approved records schedules.

To delete a record, FBI personnel must meet specific criteria and request a permanent charge out (PCO). For more information, please see the *Permanent Charge Out (Deletion) of Records From All Electronic Recordkeeping Systems* (0861D).

4.3.9.6. Expungement of FBI Records

4.3.9.6.1. Court-Ordered Expungements

CJIS must process notices regarding the modification or deletion of information contained within responsive criminal history record information (CHRI) pursuant to a court-ordered expungement and in accordance with the Controlled Substances Act (CSA), pretrial diversion, or other federal laws. Generally, these notices do not require the expungement of records within the FBI's underlying investigative case files. The exception to this general rule are notices issued pursuant to specific federal laws and accompanied by certified federal court orders.

ISS only processes expungement requests received directly from CJIS or OGC. FBI personnel must forward any expungement requests from local, state, or federal courts to CJIS's CHIPU for processing.

Expungements are accomplished through the following process:

(1) CJIS must send copies of redacted criminal history arrest record information (CHRI) prior to expungement and certified court orders requiring the expungement pursuant to the CSA, pretrial diversion, etc. to ISS via email at [redacted] b7E

(2) ISS must search the FBI's central records system indices for records in response to notices issued pursuant to 21 U.S.C. §844 (the Controlled Substance Act), pretrial diversion, or other federal laws which are accompanied by a certified federal court order and provide search results to OGC's DGC of IALB for criminal-related matters or NSCLB for national security-or cyber-related matters, within 14 days of receipt of an expungement notice from CJIS.

(3) IALB or NSCLB must review the search results and determine whether information contained within the identified investigative case files must be expunged. IALB or NSCLB must issue specific guidance to ISS as to what information must be expunged via leads set in Sentinel to [redacted] from the investigative case files. The leads must comply with the *Permanent Charge Out (Deletion) of Records From All Electronic Recordkeeping Systems Policy Directive* (0861D). IALB or NSCLB should consult and coordinate with PCLU or other OGC units, as needed. b7E

(4) ISS must review IALB or NSCLB's guidance and notify the investigative case file's case manager of the proposed redactions to the investigative case file. ISS must coordinate any concerns or objections raised by the case manager with IABLB or NSCLB.

(5) Prior to expunging records, ISS must confirm whether the associated case file has a temporary or permanent disposition. ISS must notify NARA of the court-ordered expungement prior to the destruction for files which are either unscheduled or have a permanent disposition. See 36 CFR §1226.14 for more information.

This policy does not apply to the following:

- CJIS's expungement of information maintained within the CHRI.
- Information gathered in violation of the Privacy Act (5 U.S.C. § 552a), which is covered in the *Handling of Information Gathered in Violation of the Privacy Act* (0356D).
- Routine records disposition actions authorized by the FBI's Records Retention Plan.
- Addressing, routing, dialing, signaling, or content information of wire or electronic communications acquired pursuant to consent or a state or federal court order, which may or may not be certified, that is otherwise valid on its face and issued in a matter unrelated to the expungement proceeding, unless the certified federal court order expressly references the expungement of such information.

4.3.9.7. Reporting Missing Files and Serials

FBI personnel must notify the RL within their respective office of any missing hard copy or electronic files or serials immediately upon discovery. Similarly, FBI personnel must notify their IAM of any missing electronic files or serials immediately upon discovery. The RL or IAM must report the missing file(s) or serial(s) to ISS via EC serialized to [redacted] b7E
Records Management Matters (replace XX with the office's two or three letter designator) with a lead set to [redacted] within 30 calendar days of discovery. The RL or IAM must make reasonable efforts to locate missing files or serials and must report the status of those efforts to ISS every 60 days after the initial report.

The RL must attempt to recreate any missing hard copy file(s) or serial(s) while the IAM must attempt to recreate any missing electronic file(s) or serial(s), if possible, from other sources and must reference the recreation in the new file via EC. The EC should list the recreated serial(s), as well as the sources used for recreation. The RL or IAM must notify ISS if the missing file(s) or serial(s) is subsequently located.

ISS must provide information on any missing file(s) or serial(s) to the ARO. The ARO must report to NARA any missing file(s) or serial(s) which have not been located within a reasonable time of the reported loss.

In addition to the initial reporting, the RL or IAM must immediately:

- Notify OGC's LTMS of any missing file(s) or serial(s) which contain documents subject to a legal hold, as well as any recreation efforts, and
- Report any missing hard copy or electronic file(s) or serial(s) which contain classified material or PII to their CSO. The CSO must submit a SIR via EPAS and report the

missing file or serial to the CSO Program Management Unit (CPMU) per the *Security Compliance Program Policy Guide* (0934PG).

4.3.9.8. Unauthorized Destruction of FBI Records

FBI personnel must prevent the unauthorized destruction, damage, or removal from FBI custody of hard copy records, or the deletion of electronic records from certified electronic recordkeeping systems. The unlawful removal, defacing, alteration, or destruction of federal records may result in penalties, including fines and imprisonment.

FBI personnel must immediately notify the RL within their respective office if an FBI record is destroyed, damaged, or deleted. The RL must report the destroyed, damaged, or deleted record to ISS via an EC (FD-1057), using case file [redacted] Records Management Matters (replace XX with the office's two or three letter designator) with a lead set to [redacted] within 30 calendar days of discovery. Upon receipt of the report, ISS must notify the ARO of the report. The ARO must timely report the unauthorized destruction of FBI records to NARA. b7E

4.3.9.9. Organizational Change

FBI personnel must address all nontransitory records, transitory records, and nonrecord material prior to departure. Supervisors must ensure:

- All nontransitory records have been uploaded to a certified electronic recordkeeping system and all hard copy nontransitory records have been placed in the appropriate case file;
- All transitory records and nonrecord material, which are no longer needed for business use or reference, have been dispositioned or deleted, absent a legal hold, FOIA request, or other external request;
- All transitory records and nonrecord material that are needed for business use have been moved to a location easily accessible to other FBI personnel, such as a shared drive; and
- All Sentinel cases and SharePoint sites owned by the departing personnel have been re-assigned to other FBI personnel.

FBI personnel must contact the IMD Help Desk if any hard copy records are located following an organizational change.

4.3.10. Hard Copy Case Files

FBI personnel must inventory all hard copy pending and closed case files within Content Manager and update the physical location prior to shipping files to a FBIHQ division, FO, or Legat, or to the CRC. For case files not already inventoried, FBI personnel must inventory each file and update its location in Content Manager prior to shipping. In return, the receiving office must update the file's location in Content Manager before returning any hard copy case files.

4.3.10.1. Pending Case Files

4.3.10.1.1. FBI Headquarters Files

ISS oversees the storage and maintenance of hard copy records within FBIHQ storage areas and advises on records storage and maintenance activities. FBI personnel must ensure the storage of all hard copy case files meet the minimum storage requirements. See section 4.5.1. for more information.

FBI personnel must inventory all closed case files and work with ISS before transferring hard copy case files from FBIHQ divisions to the CRC.

- **Classification 319 and 67Q Files**
    - FBI personnel must retain all administrative records covered by classifications 319 and 67Q, which relate only to individual unit activities. FBI personnel must reflect the location of the Classification 319 and 67Q files within the unit's file plan. See section 4.3.2. for more information.
- **TS and/or SCI and Special Access Program (SAP) Material**
    - FBI personnel must store all closed hard copy TS and/or SCI and SAP material in the SCIF at the CRC. Only a limited collection of TS and/or SCI and SAP records will be permitted in the IMD's SCIF at FBIHQ, J. Edgar Hoover Building (JEH) [redacted] Please contact ISS to request authorization to store material within the IMD's FBIHQ SCIF. b7E

4.3.10.1.2. Legal Attaché Files

Legats maintain pending hard copy case files within their respective office. FBI personnel must ensure the storage and maintenance of any hard copy pending case files are in compliance with SecD's Legat Support Program. The Legat Support Program ensures Legats are in compliance with FBI, Department of State, and other national requirements pertaining to secure areas, closed storage of classified information up to the SECRET classification level, and, where applicable, areas accredited as a SCIF.

FBI personnel must transfer closed hard copy Legat files to the CRC. To transfer closed case files, the LEGAT must set a lead in Sentinel to [redacted] prior to shipping files. The transport of original paper files (i.e. have not been uploaded to Sentinel) whether done in bulk or individually, must be done in accordance with Security Division requirements. The LEGAT must update the physical location of the file in Content Manager prior to shipping. b7E

4.3.10.1.3. Field Office or a Resident Agency (RA) Files

FO headquarters cities maintain pending hard copy case files within their respective office. The corresponding RA must store unclassified and classified hard copy materials in accordance with the following handling requirements:

- **TS and/or SCI material**
    - FBI personnel must not maintain TS and/or SCI materials in the RA, unless a demonstrable operational need is shown. FBI personnel must obtain approval from the Security Programs Manager (SPM) at FBIHQ, and ensure the RA storage location meets requirements for storing classified material. Please see the *Classification Management Policy Guide* (1058PG) for detailed guidance regarding classified material storage.
- **Foreign Counterintelligence (FCI), sensitive organized crime, public corruption, and undercover operation hard copy case files**
    - FCI, sensitive organized crime, public corruption, and undercover operation hard copy case files are maintained in the headquarters city, unless the SAC or ASAC determine on a case-by-case basis that the RA must retain the case file to

effectively conduct the investigation. The SAC or ASAC must document authorization and justification in an EC to the corresponding case file. SACs and ASACs are prohibited from delegating this authority. Upon receipt of the case file, RA FBI personnel must ensure it is retained in a secure manner in accordance with FBI policy.

- **CHS files**
  - FBI personnel must maintain all pending hard copy CHS case files within the FO headquarters city.

4.3.10.1.3.1. Returning Case Files to the FO

Prior to case closure, RA FBI personnel must conduct a serial-by-serial match with the original paper file and Sentinel to ensure all serials are appropriately filed including locating any and all hard copy 1A and 1C subfiles. RA FBI personnel must ensure all original serials and exhibits are included in the file before returning it to the FO. FBI personnel must not print and add copies to the hard copy case file if the record was previously imported or created through Sentinel. FBI personnel must destroy copies when no longer needed; however, the copies may constitute records and require uploading into Sentinel or another ERK system if significant notes have been added. Once digitized and uploaded, the paper copies should be destroyed in accordance with the *Importing Nontransitory Records Into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1001D). FBI personnel must follow Security Division requirements when transporting original hard copy files (i.e. those not already uploaded into Sentinel or another ERK system) in bulk or individually between FO headquarters cities and RAs and must update the physical location of files in Content Manager.

4.3.10.2. Closed Hard Copy Case Files

The FBI has centralized the location of all closed hard copy case files into the FBI's Central Records Complex (CRC) in Winchester, Virginia. The CRC utilizes ASRS technology to store and manage records. The ASRS houses inventoried closed case files with a classification of SECRET or below including those considered sensitive.

All closed hard copy case files are stored at the CRC and ASRS technology is used to store and manage records. The ASRS does not hold evidence (1B), ELSUR (1D), Federal Grand Jury (FGJ), Federal Taxpayer Information (FTI), CSAM, or closed Classification 319 or 67Q case files. Please see IMD's FAQs & Resources for a complete list of acceptable content. All hard copy Secret and Unclassified closed case files are stored in the ASRS. The only exception are those files stored in the SCIF.

To obtain access, the case manager or case participant must submit an electronic request through the FRS.

Hard copy closed case files classified as TS and/or SCI and SAP are stored in the SCIF at the CRC or FBIHQ. Any exceptions to the storage conditions must be approved by ISS' senior leadership.

4.3.10.2.1. Transferring Closed Case Files to the CRC

All FBI personnel must inventory and continue to store hard copy closed case files at or above the minimum storage standards, as set forth in 36 CFR §§1223-1238 and within section 4.5.1.1.

and 4.5.1.2. of this policy guide, until all closed case files have been fully transferred to the CRC.

FBIHQ divisions, FOs, and Legats must follow the established shipping schedule for each office until all initial transfers of closed case files have been completed.

After the initial transfer, FBIHQ divisions, FOs, and Legats must contact ISS to schedule future shipments. Prior to transfer, FBI personnel from the transferring office must:

- inventory all closed case files in Content Manager within 30 calendar days of case closure; and
- ensure closed case files do not contain physical items, contraband, or evidence. Case files containing these items will be returned to the transferring office for proper handling. See section 4.3.10.2 for more information.

FBI personnel must submit a lead request to [redacted] using the requesting office's subfile to case number [redacted] at least two weeks ahead of the intended shipping date. In the lead, FBI personnel must include the volume, classification, date span, and servicing requirements of the records. FBI personnel must also include the type of medium contained in the file, if any, in addition to paper (i.e. CD, DVD, etc.). FBI personnel must not send to the CRC any closed hard copy 319 and 67Q case files. b7E

ISS Unit Chief or designee must review the lead request and determine whether records are appropriate for storage at the CRC. ISS will give special consideration to Legat offices who may experience higher risk for maintaining certain case files. Please see IMD's FAQs & Resources for guidance on shipping records.

4.3.10.3. File Jackets

All FBI personnel must ensure the appropriate file jacket is used for maintaining hard copy case files. File jackets vary according to file content. FBIHQ division's and FO's 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
- **YELLOW (form 4-596a)** – used for files concerning personnel under investigation by the Office of Professional Responsibility (OPR)
- **BROWN (form FD-245.1)** – used for field office criminal investigative and administrative files
- **GREEN (form FD-245A)** – used for field office confidential human source (CHS) (medium green, form 245A)
- **BLUE (form FD-245b.1)** – used for all Legat office files
- **RED (form FD-245c.1)** – used for field office national security investigative files
- **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

4.4. Records Disposition

Records disposition is the development of records schedules for all agency records, the supervision and storage of inactive records, the management of the destruction of temporary records, and the transfer of permanent records to NARA. The records disposition program applies to all records created in any medium and regardless of format or enclave.

4.4.1. Records Scheduling

The ARO must develop and interpret the records schedules for all FBI case classifications and electronic information systems.

"Records scheduling" is the process of developing mandatory instructions (i.e. disposition authorities) approved by the Archivist of the United States which detail the proper handling of federal records that are no longer needed for agency business. The disposition authorities represent a legal agreement between the FBI and NARA and outline the length of time the FBI must retain records and whether the records must be destroyed or transferred to NARA.

The ARO is responsible for developing records disposition authorities for FBI records in all formats and on all enclaves. The ARO, in conjunction with system owners and FBI program managers, must review new and existing records and information systems or series to evaluate and develop appropriate retention periods and prepare disposition schedules. See the *Electronic Recordkeeping Certification Policy Guide* (0800PG) for more information.

FBI personnel should contact the ARO with any questions regarding records schedules and retention requirements for FBI records.

4.4.2. Records Retention Plan

The ARO and ISS must manage the FBI's records retention plan and provide guidance regarding the retention and disposition of nontransitory records. The records retention plan is a collection of NARA-approved disposition authorities, compiled into a set of instructions, detailing the retention and disposition of all FBI nontransitory records, regardless of location, medium, or format. Disposition schedules are broken down by records series (i.e., case classification) or, for electronic information systems, by system name. For each records series or system, the disposition schedule includes a brief description of the records, a breakdown of the types of records covered by the records series or system, and the disposition instructions.

The records retention plan:

- ensures compliance with the law;
- addresses records in all formats;
- reduces the risk records will be disposed of before meeting their authorized retention period;
- retains records for as long as needed for business purposes and disposes when no longer needed;
- facilitates discovery during litigation;
- protects the FBI from litigation resulting from the destruction of unscheduled records; and

- frees up costly office and computer space, removing records no longer needed for current business activities.

4.4.3. Creating New Records Series

FBI personnel must contact the ARO to create new records series, to obtain authorization for new case classifications, to create new electronic information systems, or to substantially change the way in which records are created and used within electronic recordkeeping systems. The ARO must work with FBI personnel to assist with these requests and to analyze retention requirements and develop retention schedules.

4.4.4. File Cutoff and Retention Period

ISS must use the file cutoff in determining the retention period for investigative and administrative case files, as well as for electronic information systems.

Similarly, FBI personnel must use the file cutoff to determine the retention period for administrative case files listed in the Classification 319 and 67Q Guide and should contact ISS to confirm the file cutoff and retention period for these files.

A file cutoff is the breaking or ending of files at regular intervals, usually at the close of the fiscal or calendar year, or after the occurrence of an event or action. The file cutoff date begins the retention period and is used in conjunction with disposition instructions to calculate the retention period for case files or electronic information systems.

- **File cutoff based on calendar or fiscal year**
    - The file cutoff cycle restarts every January or at the beginning of the fiscal year with the close of the previous year's collection and the start of the current year's collection, i.e. Classification 319 and 67Q file.
    - The IAM must annually review files contained in hard copy, on shared drives, and SharePoint sites, and determine whether files are eligible for destruction. Files with ongoing activity such as office budget, time and attendance or procurement files are examples of files with a calendar or fiscal year cutoff.
- **File cutoff based on an event or action**
    - The file cutoff is activated by the occurrence of a certain event or action which begins the retention period at the completion of the project or at the closure of an investigation.

ISS must maintain nontransitory records for the entire retention period. At the end of the retention period, ISS must destroy nontransitory records with a temporary disposition or transfer to NARA those nontransitory records with a permanent disposition.

File cutoffs are 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 the retention period. In some instances, the information system includes a history file to which inactive records are moved.

4.4.5. Disposition

4.4.5.1. Preservation of Unscheduled Records

FBI personnel are prohibited from destroying unscheduled records and must retain such records until a retention period is established and a records schedule is approved which authorizes the destruction or transfer to NARA. FBI personnel with questions should contact the ARO for assistance.

Unscheduled records are those records without a corresponding records schedule either in the FBI's records retention plan or the General Records Schedules. Unscheduled records have no authorized retention, destruction, or transfer instructions.

4.4.5.2. Nontransitory Records

4.4.5.2.1. Permanent Disposition

ISS must preserve and transfer to the National Archives all hard copy and electronic nontransitory records with a permanent disposition, absent a legal hold, FOIA request, or other external request.

Nontransitory records with a permanent disposition are records determined by NARA to have sufficient value to warrant preservation in the National Archives of the United States after expiration of the retention period.

Once transferred, NARA issues the legal transfer instrument (LTI) signifying records are the official legal property of NARA. For electronic records, ISS must delete the transferred records from the FBI's electronic recordkeeping system once NARA issues the LTI. Note: It can take several months for NARA to issue the LTI and accept legal ownership of the records.

NARA will make the transferred file available for researchers studying the FBI's investigations and activities, as appropriate and upon request. NARA will continue to apply exemptions to those records which contain classified information.

4.4.5.2.2. Temporary Disposition

FBI personnel must retain temporary hard copy and electronic nontransitory records for the entire retention period, per the applicable disposal authority, absent a legal hold, FOIA request, or other external request. Nontransitory records with a temporary disposition have insufficient value to warrant permanent preservation and are destroyed after a fixed period of time or after the occurrence of a specific event.

IMD is the only entity with authority to destroy or delete FBI records and the only entity who can authorize the destruction or deletion of the FBI's temporary nontransitory records.

The only exception are classifications 319 and 67Q case files. FBI personnel are permitted to disposition 319 and 67Q closed hard copy and electronic case files saved on their office's shared drives and on non-operational SharePoint sites, which have met the retention period and are eligible for destruction. See section 4.4.5.8 for more information.

4.4.5.3. Transitory Records

FBI personnel must routinely disposition or delete transitory records which are no longer needed for business use, or in accordance with a predetermined time period regardless of enclave or repository absent, a legal hold, FOIA request, or other external request.

FBI personnel must also disposition or delete all transitory records which are no longer needed for business use upon changing or transferring positions, retiring, or moving due to an organizational change. See section 4.1.1.2. for information on transitory records and section 4.3.9.9. on organizational change.

4.4.5.4. Nonrecord Materials

FBI personnel must routinely disposition or delete nonrecord materials which are no longer needed for reference, regardless of enclave or repository and absent a legal hold, FOIA request, or other external request. FBI personnel must manage all nonrecord material created in various repositories, network and shared drives, emails, SMS/texts, Microsoft Teams and Skype or through successor software, phone logs, and non-operational SharePoint sites regardless of enclave. See the *Managing Nonrecord Information and Information Expiration Policy Directive* (1075D).

As a matter of good recordkeeping, FBI personnel must physically separate nonrecord material from hard copy records and must readily identify, tag, and separate nonrecord material from electronic records.

FBI personnel must disposition or delete all nonrecord material prior to transferring, retiring, or moving as the result of an organizational change. See section 4.1.2.1. for information on nonrecord material and section 4.3.9.9. regarding organizational change.

To ensure proper management, FBI personnel must review information tagged as nonrecord on SCINet SharePoint and must delete nonrecord material one year after the last modification date, unless subject to a legal hold, FOIA request, or other external request.

4.4.5.5. Working Files

FBI personnel must destroy working files such as preliminary drafts, notes, and other similar materials, once the final version has been approved by an authorized FBI official and uploaded into a certified electronic recordkeeping system. See section 4.1.2.2. for more information.

FBI personnel must not destroy working files if the document is subject to a legal hold, FOIA request, or other external request.

4.4.5.6. Personal Papers

Personal papers are not federal records and must not be imported, serialized, indexed, or filed in the FBI's records management systems. FBI personnel should maintain personal files separately from official FBI records. FBI personnel must delete personal files when no longer needed for personal use, absent a legal hold, FOIA request, or other external request. See section 4.1.2.3. for more information on personal papers.

4.4.5.7. Records Pertaining to Evidence

FBI personnel must disposition all non-FBI-generated evidence upon case closure and after all investigative needs have been exhausted in accordance with the *Field Evidence Management Policy Guide* (1209PG). The disposition of non-FBI-generated evidence includes CSAM and FGJ material. See the *Crimes Against Children and Human Trafficking Program Policy Guide* (1157PG) and the DIOG for guidance.

FBI personnel must retain in the investigative case file all FBI-generated evidentiary and non-evidentiary items, regardless of size, which are documentary in nature and considered FBI

records, such as chain of custody forms, agents' notes, crime scene photographs, and laboratory analyses. These records will assume the retention period and disposition established for the investigative case file unless subject to a legal hold, FOIA request, or other external request.

4.4.5.8. Administrative Case Files: Classifications 319 and 67Q

Shared drives, non-operational SharePoint sites, and Sentinel are used to store and manage Classification 319 and 67Q case files.

The IAM must disposition 319 and 67Q closed hard copy and electronic case files stored on their office's shared drives or non-operational SharePoint sites once case files have met the retention period and are eligible for destruction. FBIHQ divisions, FOs, and Legats must not send to the CRC any closed hard copy 319 and 67Q case files.

The IAM must follow the below subsections for dispositioning classification 319 and 67Q hard copy and electronic case files. FBI personnel must contact ISS with any questions regarding the disposition of 319 and 67Q case files.

4.4.5.8.1. Administrative Case Files Stored in Hard Copy or Electronically on Shared Drives and SharePoint Sites

The IAM should destroy or delete 319 and 67Q hard copy and electronic administrative case files if there is a clear disposition authority, i.e. records schedule, which permits the destruction or deletion and the retention period has been met. Most of the FBI's 319 and 67Q administrative records have a temporary disposition and should be destroyed or deleted after expiration of the retention period. See section 4.4.4. regarding file cutoff and retention period.

Administrative records include items such as budget, time and attendance, supply, and other housekeeping functions common to all federal government offices. This guidance does not apply to administrative case files opened with an alpha designator and used for documenting non-investigative matters, i.e. 415-HQ-A123456.

To disposition 319 and 67Q case files, the IAM must:

- follow the disposition instructions provided in the Classification 319 and 67Q Guide to destroy or delete administrative records;
- not destroy or delete administrative 319 and 67Q case files where disposition has been tagged "Disposal Not Authorized," which means the file does not have a corresponding NARA-approved records schedule and is not eligible for destruction;
- check OGC's Litigation Holds/Freeze List prior to implementing disposition to ensure the case file is not subject to a legal hold or other external request; and
- document the disposition or deletion of hard copy and electronic administrative records via email or EC serialized to [redacted] (replace XX with the office's two or three letter designator). The email or EC must include the record series (i.e. case file number) and all relevant details as outlined on ISS' Information Disposition Unit's FAQs on FBINet. b7E

4.4.5.8.2. Administrative Case Files in Sentinel

Classification 319 and 67Q case files stored in Sentinel will have an automatic disposition applied through the automated records management application. IAMs must continue to

manually apply disposition to 319 and 67Q case files that are not maintained in Sentinel and stored on their office's shared drives and non-operational SharePoint sites.

Sentinel will disposition administrative records at regular intervals at the close of a calendar or fiscal year and in accordance with the closed or cutoff date. The cutoff permits the accumulation of related records within a discrete block. At the end of a specified time period, all records in the block are either destroyed or deleted if temporary or prepared for transfer to NARA if permanent, absent a legal hold, FOIA request, or other external request that would extend the retention period. ISS is responsible for the transfer of permanent administrative records to NARA.

4.4.5.9. Personnel-Related Records

Hard copy personnel subfiles already maintained at the CRC will remain at the CRC, regardless of location of FBI personnel. Disposition of subfiles Sub-M and Sub-S is established in the "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration and Addendums 1, 2, and 3" and the FBI's Records Retention Plan.

ISS must disposition unsuccessful applicant records in accordance with retention schedules absent a legal hold, FOIA request, or other external requests.

4.5. Records Protection and Records Recovery Program

FBI personnel must protect and safeguard federal records from natural or manmade events or other incidents which can damage records. All FBI personnel must understand basic records protection methods.

The following subsections provide information, guidance, and requirements for protecting and recovering records, as well as preventing and reporting a records disaster emergency.

4.5.1. Records Protection

4.5.1.1. Storage Facility Requirements

All FBI personnel must store hard copy records in accordance with 36 CFR Part 1234. The regulation outlines the minimum structural, environmental, property, and life-safety standards for all records storage facilities used by federal agencies, and those standards set forth in this PG.

The temperature and humidity levels for records storage are as follows:

Media	Temperature	Relative Humidity (RH)	Reference
Paper-based temporary records	Should not exceed 70° Fahrenheit. Ideal between 40° and 68° Fahrenheit	30-50% RH; do not exceed 50%	36 CFR §1234.14 (a)
Paper-based permanent and unscheduled records	Between 40° and 65° Fahrenheit	20-50%RH; do not exceed 50%	36 CFR §1234.14(c)
Optical – CDs/DVDs	Between 39° and 68° Fahrenheit	20-50% RH	National Institute of Standards and Technology
Microfilm/Microfiche	Should not exceed 68° Fahrenheit	35% RH (+/- 5%)	36 CFR §1238.20(a), American National Standards Institute IT9.11-1993

4.5.1.2. Common Storage Containers

All FBI personnel must store hard copy records in one of the following storage containers:

1. Vaults and fire-resistant safes offer the highest form of protection. FBI personnel must house essential records within vaults and fire-resistant safes, as essential records are critical to the continuity of FBI operations.
2. Filing cabinets are secure and the metal exterior will prevent water retention or absorption. FBI personnel must keep cabinets at least six inches off the floor; otherwise, do not utilize lower cabinet drawers for FBI records.
3. Open shelving provides more storage space. FBI personnel should ensure plastic sheeting is available to cover and protect records from water and wind damage when needed.
4. Plastic containers can protect FBI records from water more effectively than cardboard boxes; however, records stored in plastic containers are vulnerable to increased temperatures when sealed. FBI personnel must ensure plastic containers are located in a room with a lowered temperature so records inside the containers are exposed to acceptable temperature and humidity levels as set forth in 36 CFR Part 1234 and 36 CFR Part 1238.

5. Standard cardboard records storage boxes should be used for storing FBI records. The same boxes can be used for shipping files to the CRC. Banker's boxes and Xerox boxes are not acceptable protection or storage for FBI records.

With the exception of essential records, all FBI personnel must contact the IMD Help Desk and obtain approval to store hard copy records at an off-site location.

4.5.1.3. Records Disaster Preparedness

FBIHQ divisions and FOs must display emergency contact information in all areas where records are maintained. The list must include the telephone numbers for police, fire department, local emergency management agencies, and appropriate FBI COOP personnel. The same information must be recorded in each FBIHQ division's and FO's COOP plan. See section 4.6.4. for more information.

4.5.1.4. Records Protection Guidelines

To better protect and minimize risk to hard copy records, FBI personnel must:

- Store records away from any possible sources of water damage.
- Store records in file cabinets or in boxes on shelving, not directly on the floor. Boxed records must be stored at least six inches off the floor. Do not leave records exposed on desks or tables.
- Ensure records are stored in 24hr x 365 day air conditioning and not near furnaces, radiators, or heaters.
- Ensure records are not stored near hazardous material.
- Place removable hardware and CDs (or any other media containing essential records) into their protective cases when not in use.
- Duplicate and disperse essential records.
- Close and lock all drawers, file cabinets, doors, and the like in order to contain and protect essential records.
- Develop plans to protect records when notified of an impending severe weather event or other potential danger.
- Maintain an up-to-date inventory and file plan. All hard copy records must be inventoried and barcoded using the Content Manager application.

4.5.1.5. Damage to FBI Records

FBI personnel must immediately report damaged records to the IMD Help Desk and submit an EC (FD-1057) to ISS using case file [redacted] Records Management Matters (replace XX with the office's two or three letter designator). FBI personnel must ensure the EC details the incident, such as the natural or manmade event which caused the damage and a description of steps taken to remediate the damaged records. b7E

FBI personnel must understand and implement basic salvage operations to reduce the continued deterioration of FBI records damaged by natural or manmade events or causes.

IMD's Records Protection and Recovery Program intranet site provides guidance for protecting and recovering records.

4.5.1.6. Emergency Destruction of Records

FBI personnel must immediately report records which have been exposed to radiological, biological or chemical agents, or are otherwise contaminated or infested. Such records may constitute a continuing hazard to human health or to FBI property and may be eligible for emergency destruction. Other circumstances warranting emergency destruction include wartime or other national emergency conditions.

To effectuate an emergency destruction of records, FBI personnel must contact the IMD Help Desk and submit a request to ISS via an EC (FD-1057) using case file [redacted] b7E
Records Management Matters (replace XX with the office's two or three letter designator). After receipt, the ARO must notify NARA of the request and obtain approval. Upon approval, the ARO will coordinate with ISS and the requesting office for the appropriate means of destruction. ISS will generate a report detailing the records and circumstances for their destruction.

4.5.2. Records Recovery Program

4.5.2.1. IMD Records Recovery Team

The IMD Records Recovery Team is a collaborative effort of trained IMD personnel assembled to assist FBIHQ divisions and FOs with pre- and post-disaster records assistance. FBIHQ divisions and FOs must contact the Records Recovery Team for assistance during and after a natural or manmade disaster. Additional information about the Records Recovery Team can be found on IMD's Records Recovery and Recovery Program intranet site.

4.6. Essential Records and the Essential Records Program

Essential records are critical to the FBI's continued operations during and following national security emergencies or other emergency conditions. Per 36 CFR §1223.12 and FCD-1, the Essential Records Program is part of the FBI's COOP and is designed to identify critical agency records, regardless of media, and to prevent the loss of records, which could create gaps and result 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.

The Essential Records Program sets forth the procedures for identifying and protecting essential records maintained on a variety of media including paper, as well as the operational requirements during and after an emergency or disaster.

4.6.1. ERO Designation

ADs, SACs, and ADICs must designate an ERO to represent their office and to collaborate with IMD's ERP manager on all essential records policies, procedures, and programs to ensure essential records are identified, safeguarded, and maintained in accordance with established requirements.

4.6.2. Identifying and Protecting Essential Records

The ERO must review and determine which essential records are critical to FBI operations within their office during and after an emergency. Essential records include those records necessary for the protection of rights and interests of the FBI and for individuals directly affected

by the FBI's activities. Essential records fall into two categories: (1) emergency-operating records and (2) legal and financial rights records.

4.6.2.1. Emergency-Operating Records

Emergency-operating records include emergency plans, directive(s), and other authorizing issuances needed to operate the Emergency Operations Center (EOC) and its equipment. They reinforce the records recovery plans and procedures described in the COOP plan. This information includes: orders of leadership succession; delegations of authority; emergency staffing assignments with the names, addresses, and telephone numbers of the personnel and alternates assigned to the EOC, as well as those individuals who have other emergency duties or authorized access to a damaged facility to assess the extent of damage; EOC access credentials and classified or restricted access container documentation (as required); building plans and building systems operations manuals for all FBI facilities; equipment inventories for all FBI facilities; file plans describing the records series and electronic information systems maintained for all FBI facilities; copies of FBI program records needed to carry out continuing mission essential functions; and systems documentation for any electronic information systems designated as emergency-operation records.

4.6.2.2. Legal and Financial Rights Records

Legal and financial rights records are essential to protecting the legal and financial rights of the FBI and of the individuals directly affected by FBI activities. Many of these records contain PII that must be safeguarded accordingly. Formerly defined as "rights-and-interests" records, these records include: accounts receivable, Social Security, payroll, retirement, insurance, contracts, entitlements, leases, or obligations whose loss would pose a significant risk to the legal and financial rights of the federal government or persons directly affected by its actions, system documentation for any electronic information system designated to contain records needed to protect legal and financial rights, internal investigations, inspections, and active, pending, and closed litigations.

4.6.3. Contingency Planning and Risk Assessment

IMD's ERP manager must assist FBIHQ division and FO EROs with identifying and determining the critical activities within the ERO's respective office during and after an emergency or disaster. EROs must identify and preserve records which support their office's critical activities as well as the resumption of normal operations. EROs must also identify records needed to protect legal and financial rights and must determine which records are essential. IMD and the affected FBIHQ divisions and FOs must coordinate recovery efforts for essential records damaged during an emergency or disaster.

The ERP manager and EROs must evaluate the risks to records within their current locations and the medium on which they are stored, and factor the difficulty of reconstitution if such records are destroyed. The evaluation includes an assessment to determine if off-site storage should be used or if record duplication is necessary.

4.6.4. Essential Records Plans

The ERO must develop and generate a current essential records inventory, which is memorialized within the Essential Records Plan.

EROs must annually update and upload their Essential Records Plan to IMD's Essential Records Teamsite by the established deadline. EROs must not upload these plans into Sentinel.

Within the Essential Records Plan, the ERO must include a floor plan depicting where essential records are stored and located. The ERO must ensure floor plans meet the requirements set forth in Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998. Please visit the Essential Records Program intranet site for information on Essential Records Plans.

4.6.4.1. Essential Records Inventory Form

The essential records inventory form is part of the overall Essential Records Plan. The ERO must complete the form and include the following:

- The name of the office (e.g., section, unit, or squad) responsible for the record series or electronic information system containing essential information.
- The title of each record series or information system containing essential information.
- The detailed identification, including the name, location, and medium, of each record series or information system containing emergency-operating essential records or legal and financial rights essential records.
- The physical location for off-site storage of copies of the records series or information system.
- The frequency with which the essential records are to be cycled or updated.

A sample copy of the Essential Records Inventory form is available on IMD's Essential Records Program intranet site.

4.6.5. Protection Methods

When the essential records inventory is complete, the ERO, in conjunction with their respective office, must choose appropriate protection methods and storage sites for hard copy and electronic essential records. The two most common methods are (1) on-site/off-site storage and (2) duplication and dispersal of records.

4.6.5.1. Hard Copy Records

4.6.5.1.1. On-Site/Off-Site Storage

The ERO and their respective office should arrange for off-site record storage in facilities which are secure against potential emergencies or disasters. The records must remain reasonably accessible to FBI personnel. The storage site for emergency operations records may be different from the storage site for legal and financial records. For example, emergency-operating records are normally stored at a COOP site. Each office's CSO will work with members of SecD to ensure the chosen facilities possess, or are engineered to possess, security measures appropriate to the classification levels of the records stored within them.

When essential records are protected by duplication and storage at an off-site storage facility, the ERO and their respective office must take into account several considerations:

- An off-site facility may have been chosen as part of the COOP effort.

- The cost of storage will depend on the volume and format of the materials to be stored.
- Equipment, as well as electricity to run the equipment, will be needed to read digitized records.
- Copies of emergency-operating records must be stored in an off-site facility that is accessible to the appropriate FBI personnel 24 hours a day.
- Copies of essential records must be stored at an off-site facility in accordance with NARA regulations, Title 36 CFR Part 1234. SCIFs must be used to store TS and/or SCI and must meet the requirements of Intelligence Community Directive (ICD) 704.
- The on- and off-site facilities must have temperature and humidity controls and 24-hour security.
- The on- and off-site facilities must have sprinkler systems or smoke detection systems that alert emergency officials when activated, and these areas must have one or more fire extinguishers.
- The facilities should have equipment to reproduce records.
- The on- and off-site areas where essential records are stored must be inspected for water leaks or other potential hazards at least annually.
- The on- and off-site areas where essential records are stored must not be located in designated flood plains.

The disadvantage to keeping essential records solely on-site is the potential for total or near total destruction or contamination in the event of a disaster. Therefore, storing copies off-site is an important aspect of essential records maintenance.

If off-site storage is not an option, each office must protect essential records by storing them in fire-resistant vaults, safes, or file cabinets. Such equipment is rated according to the maximum number of hours of exposure to fire and the maximum exposure temperature the equipment can withstand.

- Fire resistant cabinets and safes are best for small quantities of active essential records, where ease of accessibility is needed.
- Vaults are used for larger quantities of records. These devices must be in buildings with sprinkler systems or smoke detection systems that alert emergency officials when activated. All containers must be General Services Administration (GSA)-approved for the classification levels of the records stored.
- The National Fire Protection Association classifies records protection equipment into two elements: (1) time in hours and (2) interior temperature limit. Time limits range from one-half hour to four hours. This means the equipment must sustain sudden exposure to high temperatures, to the extent described in the requirements, without igniting. The selected interior temperature limit will be determined by the contents:
    - Paper: 350 degrees Fahrenheit
    - Photographs: 150 degrees Fahrenheit
    - Electronics: 125 degrees Fahrenheit

- Areas where essential records are stored must be inspected for water leaks at least annually. Inspections can be completed by personnel assigned to those areas. The facility must be inspected annually for insect and rodent infestation.
- There must be an evacuation plan that is tested annually at the emergency facility, and emergency lights must also be installed and tested annually.

Magnetic tape, microfilm, removable hardware, diskettes, CD-ROMs (compact disc + read only memory), and photographic records require special equipment because of their susceptibility to high humidity. The FBI follows NARA recommendations concerning records storage of these types of materials. The IMD Essential Records Program intranet site contains additional information about storing records.

Periodic cycling of essential record copies is critical. The FBI determines cycling frequencies based on how current the emergency-operating, legal and financial rights records must be in order to meet their information responsibilities. Depending on the need and the medium on which an essential record is maintained, cycling may occur daily, weekly, monthly, annually, and so on.

4.6.5.1.2. Duplication and Dispersal

The duplication and dispersal technique involves the routine or planned distribution of duplicate copies of essential records to locations other than the duty station. During the regular course of business, duplicates of essential records are routinely distributed to alternative sites, specifically for protection purposes. The primary copy is the essential record; the duplicates are considered essential record security copies. If the primary copy is destroyed or otherwise unusable, the essential record security copy then becomes the primary record. Unless subject to a legal hold, the duplicates (security copies) are sent to designated locations and are maintained for the same retention period as the primary essential records.

Dispersal requires constant monitoring by each office's ERO to ensure the essential record security copy is updated periodically. Duplicates must be dispersed to locations that will not be affected by an area-wide disaster that could destroy both duplicates and the primary record, yet close enough to be readily accessible, if needed. In addition, each office's ERO must update and upload the Essential Records Plan to the IMD Essential Records Program Intranet site annually. EROs should update their ERPs within their respective division's or office's folder on the designated SharePoint site as needed to ensure the most current Essential Records Plans are made available. This should be done in addition to the annual requirement.

4.6.5.2. Electronic Records

The protection of electronic essential records poses its own challenges because of the need to consider not only the record, but also the hardware, software, and system documentation. Each office must, at least annually, save its essential electronic records to the FBI local area network (LAN) servers in routine backup rotations or make backup copies of essential electronic records on floppy discs, magnetic tape, removable hardware, or CD-ROMs/DVD-ROMs (digital video [versatile] disc + read only memory), or on the most current technological media, to be stored at alternative off-site locations. The office's ISSO or, in their absence, the CSO, must be consulted regarding electronic records storage and protection.

4.6.6. Training

All ADs, SACs, and ADICs must ensure EROs and FBI personnel assigned responsibilities in the essential records program receive appropriate training.

EROs must provide periodic briefings to senior managers, especially those new to the FBI, about FBI records and their relationship to the Essential Records Plan.

All ADs, SACs, and ADICs must ensure employees receive training in identifying, inventorying, protecting, storing, and cycling essential records. Essential records training should be integrated into existing FBI training, particularly in such areas as records management and emergency coordination.

ERP manager must maintain ERP procedures, updates, and training materials on IMD's Essential Records Program Intranet site.

4.6.7. Review and Testing

In accordance with mandatory COOP requirements and in conjunction with SecD's CPMU, the ERM must conduct periodic reviews to determine if the FBI's essential records and copies of essential records are current, adequately protected, and readily available to appropriate FBI personnel.

Federal agencies, including the FBI, are required to test their emergency plans and procedures periodically to determine if records designated as essential allow agency personnel to function effectively during an emergency. After the test, the managing official of the FBIHQ division or FO should meet with test participants to assess the results and make appropriate modifications. Testing should be conducted in conjunction with the FBIHQ division's or FO's CSO and SecD.

Per Federal Continuity Directive (FCD)-1, *Federal Executive Branch National Continuity Program and Requirements Annex I Essential Records Management*, federal agencies must annually test the capabilities for protecting classified and unclassified essential records, and for providing access from alternate facilities.

5. Summary of Legal Authorities

Several agencies, including NARA, the Office of Management and Budget (OMB), and the GSA share oversight of records management in the federal government. Listed below are citations to the codes, regulations, and authorities most relevant to records management:

- Records Management by the Archivist of the United States and by the Administrator of General Services (44 U.S.C. Chapter 29)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Disposal of Records (44 U.S.C. Chapter 33)
- Coordination of Federal Information Policy (44 U.S.C. Chapter 35)
- Public Money, Property, or Records (18 U.S.C. §641)
- Criminal Penalties for Unauthorized Disposal of Federal Records (18 U.S.C. §2071)
- The Freedom of Information Act (5 U.S.C. §552)
- The Privacy Act of 1974 (5 U.S.C. §552a)
- Federal First Offender Act (18 U.S.C. §3607)
- Controlled Substances Act (CSA) (21 U.S.C. §844)
- Federal Records (36 CFR Chapter 12, Subchapter B)
- Personnel Records (5 CFR Part 293)
- EO 12656 (Assignment of Emergency Preparedness Responsibilities)
- EO 10346 (Responsibility for Mission Critical Functions)
- EO 13228 (Office of Homeland Security and the Homeland Security Council)
- EO 13231 (Critical Infrastructure Protection in the Information Age)
- OMB Circular A-130: Management of Federal Information Resources
- OMB M-19-21: Transition to Electronic Records
- U.S. Office of Personnel Management (OPM) Manual, The Guide to Personnel Recordkeeping (June 1, 2011)
- FCD-1: Federal Executive Branch National Continuity Program and Requirements, Annex F, January 17, 2017
- FCD-2: Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process, June 13, 2017
- *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom), dated December 1, 2008.
- Department of Justice Order No. 0801, March 12, 2014 (Records and Information Management)

- Department of Justice Policy Statement 0801.02, December 18, 2014 (Removal of and Access to DOJ Information)
- Department of Justice Instruction 0801.04.01 (January 18, 2017) (Electronic Mail Retention)
- Department of Justice Instruction 0801.04.02 (December 11, 2019) (Electronic Messaging Records Retention Instruction)
- United States Attorneys' Manual (USAM) Title 9-22.000, "Pretrial Diversion Program"

Appendix A: References

The bulleted list of references below provide contextual information for this policy. See the IMD Intranet site for additional information.

- *Construction Requirements and Specifications for Approval of Open- and Closed-Storage Secure Areas Policy Guide* (0713PG)
- *Declassification of Classified National Security Information Policy Guide* (0839PG)
- Department of Justice (DOJ) Order 2710.10A, Federal Court Orders for the Disposition of Official Records Other Than Under the Controlled Substances Act
- *Domestic Investigations and Operations Guide (DIOG)*
- *Electronic Recordkeeping Certification Policy Guide* (0800PG)
- *Emergency Preparedness and Continuity of Operations Policy Guide* (1084PG)
- *FBI Ethics and Integrity Program Policy Guide* (1120PG)
- FBI records retention plan and disposition schedules for pre-universal case file numbers (NC1-65-82-04)
- FBI records retention plan and disposition schedules for universal case file numbers (N1-065-04-4)
- FBI records disposition authority for director's office records (N1-065-07-1)
- *Field Evidence Management Policy Guide* (1209PG)
- *Freedom of Information Act and Privacy Act Requests* (1027D)
- Guidelines for SharePoint Records and Information Management (RIM) Intranet site
- *Handling of Information Gathered in Violation of the Privacy Act* (0356D)
- IMD Help Desk
- *IMD Statement of Authorities and Responsibilities* (0457D)
- Information Management Division Intranet site
- *Importing Nontransitory Records Into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1001D)
- Indexing User Manual for Sentinel
- Intelligence Community Directive (ICD) 704
- ISS Intranet Site
- *Legal Hold Policy* (0619D)
- "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration" and Addendums 1, 2, and 3
- National Fire Protection Association (NFPA) Web site http://www.nfpa.org/

- Open storage secure area checklist
- *Permanent Charge Out (Deletion) of Records From All Electronic Recordkeeping Systems* (0861D)
- *Physical Security for Sensitive Compartmented Information Facilities Policy Guide* (1107PG)
- *Prepublication Review Policy Guide* (1065PG)
- *Preservation and Disclosure of Electronic Communications in Federal Criminal Cases Policy Directive* (0423D)
- *Privacy Policy Guide* (1113PG)
- *Security Compliance Program Policy Guide* (0934PG)
- Sentinel Intranet site
- WSU Intranet site

Appendix B: Definitions and Acronyms

Definitions

Content administrator: the content administrator represents an FBIHQ division's, FO's, or Legat's FBI Network (FBINET) (SECRET Enclave) interests and FBINET site(s) at large. The content administrator is responsible for maintaining user access privileges on behalf of the division, FO, or Legat and oversees and ensures that all policies, rules, and guidance governing FBINET sites are correctly applied. The content administrator may also manage, produce, or own content.

Content manager: the individual responsible for the publishing, editing, and modifying of content, as well as site management.

Content management: the administration of content throughout its life cycle from creation to permanent storage or deletion. When stored and accessed via computers, this information has come to be referred to simply as content or digital content. The content involved may be images, videos, audio, and multimedia, as well as text.

Contingency planning: instituting policies and procedures to mitigate the effects of potential emergencies or disasters on an agency's operations and records. Contingency planning is part of the continuity of operations planning required under federal preparedness circulars and other guidance issued by the Federal Emergency Management Agency (FEMA) and EO 12656.

Criminal history record information: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

Cutoff: the breaking or ending of files at regular intervals, usually at the close of the fiscal or calendar year, or after the occurrence of an event or action. It enables the disposal or transfer of files in blocks and permits the establishment of new files. The cutoff date is used in conjunction with the disposition instructions to determine the retention period.

Cycle: the periodic removal of obsolete copies of essential records and their replacement with copies of current essential records. This may occur daily, weekly, quarterly, annually, or at other designated intervals.

Decommissioning: the process of removing a SharePoint site from active servers. Also refers to the process of closing down information systems.

Disaster: an unexpected incident inflicting destruction and distress and having long-term, adverse effects on agency operations. Each federal agency defines what constitutes a long-term, adverse effect in relation to its most critical program activities. See emergency.

Disaster preparedness testing: periodic application of the disaster plan under a controlled practice situation. Tests help identify weaknesses in the plan and allow the disaster team to evaluate the plan's potential effectiveness during an emergency.

Digital born: materials that originate in an electronic form.

Dispersal: protection of essential records through the production of duplicate copies in order to store data at other locations and/or levels of an organization.

Disposition: includes the development of retention schedules for all records, supervision of the storage of inactive records, the destruction of temporary records, and the transfer of permanent records to NARA.

Duplication: transferring of records to microfilm, electronic or magnetic media, or paper photocopies in order to protect essential information. Copies are made at the time of origin or on a scheduled basis.

e-Discovery: refers to discovery in civil and criminal litigation of information possessed in electronic form. This includes, but is not limited to, emails, attachments, and other data stored on a computer, network, backup, or other storage media.

Electronic information system: a system that contains and provides access to computerized Federal records and other information.

Electronic messaging tools: technologies used to facilitate the exchange of information and to allow FBI personnel to share, discuss, and collaborate on information, ideas, projects, and activities. Electronic messaging tools encompass both (1) point-to-point communication tools such as emails, instant and text messaging, digital and wireless phone calls, voicemail, Voice over Internet Protocol (VoIP), online and audio meeting and conferencing, and (2) web-based tools such as shared mail services (e.g. shared calendars), video and photo-sharing sites, virtual bulletin boards, wikis, blogs, and professional- and social-networking sites.

Electronic records: any information recorded in a form that 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 that the agency determines is required to meet agency business needs (36 CFR §1220.18).

Electronic recordkeeping system: an electronic information system approved to manage records received, created, or stored in digital format for their approved retention period.

Emergency: a situation or an event of a serious nature, developing suddenly and unexpectedly, and demanding immediate action. An emergency is of short duration—an interruption of normal agency operations for a week or less. It may involve electrical failure or minor flooding caused by broken pipes.

Emergency-operating records: the type of essential records necessary for the continued functioning or reconstituting of an organization during and after an emergency. Included are emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, select program records needed to continue the most critical agency operations, and related policy or procedural records that assist agency personnel in conducting operations under emergency conditions and assist in resuming normal operations following an emergency.

Essential records: critical agency records which are needed to meet operational responsibilities under national security emergencies or other emergency conditions or to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records).

Essential records inventory: a detailed listing of essential records included in an Essential Records Plan. It provides the name of the division or office responsible for the essential records

series or electronic information system, the title of each essential records series or information system, the identification of each essential records series or information system as either an emergency-operating or a legal and financial rights series or system, the identification of the medium and storage location of each essential records series or information system, and the frequency with which the essential records series or electronic information systems are to be cycled (see identification [selection] of essential records and inventory).

Essential Records Program: the policies, plans, and procedures developed and implemented to protect the essential records needed to meet operational responsibilities under national security or other emergency or disaster conditions. It includes the resources needed to identify, use, and or to protect the government's rights and those of its citizens. It is a program element of an agency's emergency management function.

Expungement: the physical removal and destruction of a record or a portion of a record or, depending on a certified federal court order and a governing statute or program, the removal, sealing, and secure storage of records.

FBI investigative case file: a repository of investigative records in criminal and national security law investigations.

FBI Personnel: any individual employed by, detailed to, or assigned to the FBI, including task force officers, members, and participants; members of the armed forces; experts or consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors; personal service contractors of the FBI; or any persons who act for, or on behalf of the FBI, as determined by the FBI Director.

Federal Records Center: a center established, maintained, and operated by NARA under authority of 44 U.S.C. §2907 for the storage, processing, and servicing of federal agencies' records.

File plan: (1) a plan designating the physical location(s) at which an agency's files are to be maintained, the specific types of files to be maintained there, and the organizational element(s) having custodial responsibility; (2) a document containing the identifying number, title or description, and disposition authority of files held in an office.

Hard copy: a physical document, such as paper or microfilm.

Information Asset Manager: an employee, organizationally, at the unit or squad level, who collaborates with members to ensure their entity's information assets are managed in accordance with records management laws, regulations, and guidelines.

Inventory: (1) a survey of agency records and nonrecord materials conducted primarily to develop records schedules and to identify various records management problems, such as improper applications of recordkeeping technology; (2) the results of such a survey; (3) in archives administration, a type of finding aid for accessioned permanent records (see essential records inventory).

Legacy files: case files in the Automated Case Support (ACS) system which migrated into Sentinel.

Legal and financial rights records: the type of records necessary for protecting the legal and financial rights of the government and of the individuals directly affected by its activities. These records were formerly defined as "rights-and-interests" records. Examples include accounts

receivable records, social security records, payroll records, retirement records, and insurance records. Records having the properties of both emergency-operating and legal and financial rights records are treated as emergency-operating records.

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

Legal transfer instrument: formally conveys the legal custody of a records transfer to NARA. It is automatically created by the Electronic Records Archives (ERA) system.

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 that describes and gives information about other data, such as how, when, where, and by whom a particular set of data was collected or how the data is formatted. For example, author, date created, date modified, file size.

Mid-volume or high-volume scanner: a document scanner that provides the capability for scanning above 75 double-sided PPM.

Mitigation: any action taken to prevent or reduce the effects of a man-made or natural disaster.

National security emergency: any event, natural disaster, military attack, technological emergency, or other emergency that seriously degrades or threatens the national security of the United States, as defined in EO 12656.

Nonrecord material: U.S. Government-owned documentary materials excluded from the legal definition of records and includes unofficial copies of documents kept only for convenience or reference, stocks of publications, and library or museum material intended solely for reference or exhibition.

Nontransitory record: a record needed for more than 180 days and possesses one or more of the following characteristics: contains information necessary to adequately and properly document the activities and functions of the agency; provides documentation of agency decisions and commitments reached orally (person-to-person, phone, video, or in conference); conveys information of value on agency activities and adds understanding of agency operations and responsibilities; documents the formulation and execution of policies and decisions; and/or provides proof of fiscal or legal rights and obligations.

Off-site storage: a facility other than an agency's normal place of business where inactive records are stored; for example, the CRC provides off-site storage for closed case files. Also refers to a storage location for essential records to ensure they are not subject to damage or destruction from an emergency or a disaster affecting an agency's normal place of business.

Personal papers: documentary materials, belonging to an individual, which are not used to conduct official agency business. It relates solely to an individual's personal and private affairs or are used exclusively for that individual's convenience. It can exist in any format or medium such as SMS/text and electronic instant messages, email, and voicemail.

Program managers: those people responsible for specific functions within an agency, such as data processing or payroll.

Protective methods: (1) techniques for ensuring the continued survival of essential records. These include designating existing duplicates of essential records as essential records copies;

preparing duplicates of original records in their original medium (e.g., paper copies of paper originals); or preparing duplicates of original records in an alternate medium (e.g., microfiche copies of electronic originals); (2) secure storage, duplication, or relocation methods used to suitably protect essential records; (3) types of special protective measures, including, fire-rated filing equipment, on-site vaults, transfer of records to offsite storage, and duplication of records.

Record: 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.

Recorded information: this term, as used in the records definition, 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 Recovery Team: IMD team responsible for overseeing the FBI's Records Recovery Program. The RRT members are trained to respond appropriately during a disaster for the preservation and recovery of records.

Records retention plan: a document providing mandatory instructions for what to do with records (and nonrecord materials) no longer needed for current business. The plan provides authority for the disposal of temporary records and the transfer of permanent records to the National Archives. Also referred to as a records control schedule.

Risk assessment: a method of analyzing the impact on an agency due to the loss of records.

Scanner: a document conversion device that converts hardcopy format into electronic format.

Senior officials: individuals within an organization responsible for the agency and program policy- and mission-related actions. The FBI's senior officials include the director, deputy director, associate deputy director, and executive assistant directors.

Series: file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship by their creation, receipt, or use. This is also called a record series or a file series.

SharePoint site: a digital or electronic collection of pages, lists, and libraries configured for achieving a specific goal. A site may contain subsites, which may include further subsites having navigation, themes/branding, custom permissions, workflows, and the ability to be configured or customized in various ways. SharePoint sites may contain both record and nonrecord materials.

Site owners: FBI personnel, assigned by a FBIHQ division, FO, or Legat who are responsible for the SharePoint site. The site owner can assign access permissions, create lists and libraries, and must agree to the decommissioning of the SharePoint site.

Stub record: serves as a placeholder to document the removal of serial. The placeholder assumes the original serial number, is substituted for the deleted serial or text and will remain in the system until final disposition of the case file.

System documentation: records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, codebooks, record layouts, user guides, and output specifications.

System of records: a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. This term is specific to the Privacy Act of 1974 and not applicable under the Federal Records Act.

System owner: a term referring to program managers and business owners who manage the acquisition or development of an electronic information system or places an electronic information system into operation. Within the FBI, the CIO and each AD is responsible for the operational management of applications or electronic information systems that directly support his or her business area.

Transitory record: a temporary record that is: (1) needed for a short time, generally less than 180 days and (2) is not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Both criteria must be met for the record to be transitory.

Working files: preliminary drafts and other similar materials, regardless of medium, which have not been approved by an FBI official with authority.

Acronyms

AD	assistant director
ADD	associate deputy director
ADIC	assistant director in charge
AOR	area of responsibility
ARO	agency records officer
ASAC	assistant special agent in charge
ASRS	Automated Storage and Retrieval System
BA FO	Baltimore field office
BSS	Biometric Services Section
CCR	change case request
CD-ROM	compact disc-recordable
CFR	Code of Federal Regulations
CHIPU	Criminal History Information and Policy Unit
CHRI	Criminal History Record Information
CHS	confidential human source
CJIS	Criminal Justice Information Services Division
CMAU	Critical Mission Assurance Unit
COOP	Continuity of Operations Program
CPMU	Chief Security Officer Program Management Unit
CRC	Central Records Complex
CSA	Controlled Substances Act
CSAM	child sexual abuse material
CSO	chief security officer

DD	deputy director
DGC	deputy general counsel
DIOG	*Domestic Investigations and Operations Guide*
DOJ	Department of Justice
DVD-ROM	digital video [versatile] disc + read only memory
EAD	executive assistant director
EC	electronic communication
e-Discovery	electronic discovery
EIM	Enterprise Information Management
EO	executive order
EOC	Emergency Operations Center
eOPF	electronic official personnel folder
EPAS	enterprise process automation system
ERA	essential records archives [system]
ERKC	Electronic Recordkeeping Certification
ERO	essential records officer
ERP	essential records program
EVC	Enterprise Vetting Center
Exec Sec	Executive Secretariat
fax	facsimile
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FBINET	FBI Network [SECRET enclave]
FCD	federal continuity directive

FCI	foreign counterintelligence
FGJ	Federal Grand Jury
FO	field office
FOIA	Freedom of Information Act
FRS	file request system
FTI	Federal Taxpayer Information
GSA	General Services Administration
HR	human resources
IALB	Investigative and Administrative Law Branch
IAM	Information Asset Manager
ICD	Intelligence Community directive
IMD	Information Management Division
ISS	Information Services Section
ISSO	information system security officer
IT	information technology
ITADD	Information Technology Applications and Data Division
ITB	Information and Technology Branch
ITMS	Information Technology Management Section
LAN	local area network
LEGAT	legal attaché [head of office]
Legat	legal attaché [office]
LitB	Litigation Branch
LSS	Language Services Section
LTI	legal transfer instrument

LTMS	Litigation and Technology Management Section
MFP	multifunction printer
MSS	Mission Support Services
NARA	National Archives and Records Administration
NFPA	National Fire Protection Association
NNCP	National Name Check Program
NSCLB	National Security and Cyber Law Branch
NVC	National Vetting Center
OCIO	Office of the Chief Information Officer
OCR	optical character recognition
OGA	other government agency
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OO	office of origin
OPA	Office of Public Affairs
OPR	Office of Professional Responsibility
PA	Privacy Act
PAR	performance appraisal report
PCLU	Privacy and Civil Liberties Unit
PCO	Permanent Charge Out (deletion)
PG	policy guide
PII	personally identifiable information
PPM	pages per minute
PDF	Portable Document Format

RA	resident agency
RIDS	Records/Information Dissemination Section
RL	records liaison
RMA	records management application
RMT	records marking tool
SA	special agent
SAC	special agent in charge
SAP	special access program
SCINet	Sensitive Compartmented Information Network (TS/SCI Enclave)
SCIF	Secure compartmented information facility
SecD	Security Division
SF	standard form
SIR	security incident report
SPM	security programs manager
TIS	Technology Innovation Section
TS	top secret
USAM	United States Attorneys' Manual
U.S.C.	United States Code
USIC	United States Intelligence Community
VoIP	voice over internet protocol
WSU	Web Services Unit