FEDERAL BUREAU OF INVESTIGATION

POLICY DIRECTIVE

Managing Nonrecord Information and Information Expiration Policy Directive 1075D

General Information

Proponent	Information Management Division (IMD)
Publication Date	2019-08-22
Review Date	2022-08-22
Last Updated	N/A
Supersession	None

1. Authorities

- Title 44 United States Code (U.S.C.) Chapters 29, 31, and 33 (Records Management)
- Title 44 U.S.C. Chapter 36 (Management and Promotion of Electronic Government Services)
- Title 36 Code of Federal Regulations (CFR) Chapter 12, Subchapter B (Records Management)
- Office of Management and Budget (OMB) M-19-21, "Transition to Electronic Records" (June 28, 2019)
- Department of Justice (DOJ) Order 0801, *Records and Information Management* (March 12, 2014)
- DOJ Order 0801.04 *Electronic Mail Records Retention* (September 21, 2016)

2. Purpose

This policy addresses the Federal Bureau of Investigation's (FBI) overarching Enterprise Information Management (EIM) strategy to manage all nonrecord information currently held outside of certified electronic recordkeeping systems. For questions regarding certified electronic recordkeeping systems, e-mail the Records Management Application Unit (RMAU) at [redacted] b7E

3. Scope

This policy applies to all FBI personnel.

4. Exemptions

4.1. Foreign Intelligence Surveillance Act (FISA)-acquired information or information subject to legal holds, investigations, Freedom of Information and Privacy Act (FOIPA)

requests, or special inquiries of any kind, including other legally binding requirements that mandate a retention period beyond the time frame specified in this policy, are exempt.

4.2. Information held in a certified electronic recordkeeping system, such as Sentinel, Delta, Guardian, or successor systems, is exempt from this policy.

5. Policy Statement

5.1. As a standard practice, nonrecord information must be dispositioned (deleted) by the creator or the recipient when no longer needed for business use.

5.2. If nonrecord material is not dispositioned (not deleted) by either the creator or the recipient when no longer needed, an EIM process will identify and delete the following nonrecord information five years from the accessed or modified date, whichever is later, for documents and files and five years from the sent or received date for electronic communications:

5.2.1. All nonrecord information contained and stored in various repositories, including, but not limited to, network or shared drives. The five-year disposition for nonrecord information is reset when the document or file is accessed or modified.

5.2.2. All nonrecord information generated on any enclave as communication information, including, but not limited to, e-mails, short message service (SMS)/texts, Lync (Skype for Business), and phone logs, regardless of storage repository.

5.2.3. All nonrecord information stored on nonoperational SharePoint sites. (See the *Records Management Requirements for the Creation, Maintenance, and Decommissioning of SharePoint Sites Policy Directive* [0768D] for information on operational sites.)

5.3. Nonrecord information placed on removable electronic storage (RES) must be managed by the information owner until the EIM process is practicable for external devices.

6. Roles and Responsibilities

6.1. All FBI personnel must:

6.1.1. Ensure that all record information is appropriately uploaded to an approved electronic recordkeeping system prior to the five-year disposition of nonrecord information. (See the *Records Management Policy Guide* [0769PG], subsection 2.8.)

6.1.2. Perform disposition (deletion) of nonrecord information when that information is no longer needed for business use.

6.2. IMD must:

6.2.1. Set forth and manage an EIM strategy across all enclaves and repositories to reduce costs and risks, while realizing the full value of the FBI's information assets.

6.2.2. Develop and maintain standard practices and processes to ensure that information is generated and managed in alignment with the EIM strategy.

6.2.3. Collaborate with the Information Technology Branch (ITB) and the Office of the Chief Information Officer (OCIO) to ensure that information owners are alerted when disposition (deletion) will be enacted.

6.2.4. Ensure that proper information management (IM) compliance audits and checks align with the requirements of this policy.

6.2.5. Train and communicate the new IM framework so that FBI personnel are equipped with the tools needed to understand and apply EIM practices in all aspects of their work.

6.2.6. Collaborate with Federal Bureau of Investigation Headquarters (FBIHQ) divisions and field offices (FO) on implementation of the EIM process.

6.3. OCIO must:

6.3.1. Develop enterprise processes for managing nonrecord information across all enclaves.

6.3.2. Evaluate and enhance new and existing technologies across all enclaves and collaborate with information technology (IT) service providers to implement the functionality necessary to ensure compliance with this policy's requirements.

6.3.3. Establish IM standard practices to be implemented across the enterprise by IT service providers, as well as update business processes to ensure compliance with the policy.

6.3.4. Ensure that IM services for all FBI users do not create additional administrative burdens or encourage users to develop noncompliant alternative methods.

6.4. ITB/ Science and Technology Branch (STB)/IT service providers must, in conjunction with OCIO and IMD, ensure that disposition functionality is incorporated throughout the enterprise.

6.5. Systems owners must:

6.5.1. In conjunction with OCIO, develop and maintain processes for managing nonrecord information in accordance with this policy.

6.5.2. In conjunction with IMD, assess systems for Electronic Recordkeeping Certification (ERKC) to determine their ability to manage record and nonrecord information.

7. References

7.1. *Records Management Policy Guide* (0769PG)

7.2. *Records Management Requirements for the Creation, Maintenance, and Decommissioning of SharePoint Sites Policy Directive* (0768D)

7.3. *Records Management User Manual*

7.4. *Electronic Recordkeeping Certification Policy Guide* (0800PG)

7.5. *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide* (0828PG) [leads to a ~~SECRET//NOFORN~~ document]

8. Definitions and Acronyms

8.1. Definitions:

8.1.1. 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.

8.1.2. IT service provider: an organization or a group that provides and manages IT solutions and/or services to end users.

8.1.3. Nonrecord: A nonrecord contains no documentary or evidentiary value to the business of the FBI and does not require retention beyond its useful life, as determined by either the creator or the recipient, unless subject to an external request or a legal hold. Examples of nonrecord materials include library materials made or acquired and preserved solely for reference or exhibition purposes, stocks of publications or unprocessed blank forms, or extra copies of documents preserved only for convenience of reference. (Not all copies are nonrecord materials. Copies of nonrecords may be used for different purposes within the FBI, and they may take on record status. For example, copies of other government agency [OGA] records may be maintained by the FBI as records. A nonrecord copy may also become a transitory record or a nontransitory record if substantive notes or comments are added to the document.)

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

8.1.5. 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 (USG) or because of the informational value of data in them. Records do not include library or museum materials made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. Section [§] 3301.)

8.1.6. Removable electronic media: portable, electronic storage media, such as magnetic, optical, and solid-state devices that can be inserted into, and removed from, a computing device and that are used to store and transfer text, video, audio, and image information. Such devices have no independent processing capability. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, and similar Universal Serial Bus (USB) storage devices.

8.1.7. System owner: a broad term referring to anyone who manages the acquisition or development of an electronic information system or places an electronic information system into operation. Within the FBI, the chief information officer (CIO) and each assistant director (AD) is responsible for the operational management of applications or electronic information systems that directly support his or her business area.

8.1.8. Transitory record: a temporary record that has only minimal documentary or evidentiary value and is needed for 180 calendar days or less.

8.2. Acronyms:

AD	assistant director

CIO	chief information officer
CFR	Code of Federal Regulations
DOJ	Department of Justice
EIM	Enterprise Information Management [strategy]
ERKC	Electronic Recordkeeping Certification
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FISA	Foreign Intelligence Surveillance Act
FO	field office
FOIPA	Freedom of Information and Privacy Act
IM	information management
IMD	Information Management Division
IT	information technology
ITB	Information Technology Branch
OCIO	Office of the Chief Information Officer
OGA	other government agency
OMB	Office of Management and Budget
PD	policy directive
RES	removable electronic storage
RMAU	Records Management Application Unit
SMS	short message service
STB	Science and Technology Branch
USB	Universal Serial Bus
U.S.C.	United States Code
USG	United States government

Approvals	
Sponsoring Executive Approval	
Name	**Title**
Marlin L. Ritzman	Assistant Director Information Management Division
Final Approval	
Name	**Title**
Paul M. Abbate	Associate Deputy Director