REQUEST FOR RECORDS DISPOSITION AUTHORITY	JOB NUMBER
	N1-065-06-1
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001	Date received 9-19-2005
1. FROM (Agency or establishment) **DEPARTMENT OF JUSTICE**	**NOTIFICATION TO AGENCY**
2. MAJOR SUBDIVISION **FEDERAL BUREAU OF INVESTIGATION**	In accordance with the provisions of 44 U.S.C. 3303a, the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.
3. MINOR SUBDIVISION **CRIMINAL JUSTICE INFORMATION SERVICES DIVISION**	

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE NUMBER	DATE	ARCHIVIST OF THE UNITED STATES
Teresa C. Sharkey, CRM	**202-324-1613**	4/19/07	Allen Weinstein

6. AGENCY CERTIFICATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached 3 page(s) are not needed now for the business for this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies,

☒ is not required ☐ is attached; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
9/12/05	William L Hooton	Assistant Director

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	The attached pages provide disposition instructions for records relating to **Law Enforcement Online (LEO)**, which is a dynamic portal for participating agencies to exchange information, partake in on-line educational programs, and engage in professional special interest and topically focused dialogue.		

SA Copies Sent to Agg/NWMD/NWMCW

Law Enforcement Online (LEO)

OVERVIEW

Law Enforcement Online (LEO) is a dynamic portal for participating agencies to exchange information, partake in on-line educational programs, and engage in professional special interest and topically focused dialogue. Since its development in 1995, LEO has enabled real-time communications and information sharing for a community currently comprised of 42,000 users who are employed by Federal, state and local agencies.

The primary function of LEO is to serve as an online portal that provides the following services:

- Native Services that are basic services to all users, such as electronic mail (e-mail), e-learning, access to LEO Special Interest Groups (LEOSIGs), chatting capabilities through Internet Relay Chat (IRC), search capabilities, and news groups that contain electronic bulletin boards (e-bulletin boards).
- Hosted Services that have their own databases and/or applications for storing and retrieving information specific to a topic of interest and are a means to collect and disseminate information.
- Portal Services that provide connectivity to remote law enforcement systems that are not housed or maintained on the LEO network. (Connections are made via a WAN or secured internet link.)

SYSTEM OPERATIONS AND MANAGEMENT RESPONSIBILITY

The FBI's Criminal Justice Information Services (CJIS) Division, Program Support Section (PSS), Program Management Office (PMO), is responsible for managing and administering LEO. To accomplish these responsibilities, PMO utilizes FBI employees, employees of participating agencies, and Louisiana State University (LSU) to perform system operation and management functions.

CONTENT RESPONSIBILITY

LEO's content includes web pages and linked documents or files that are available for users to view, print or download. The FBI executes an Interconnectivity Security Agreement (ISA), Memorandum of Understanding (MOU), and/or an Electronic Communication (for internal connectivity between FBI Divisions) with each participating entity. In accordance with the agreements, databases and applications (systems) that are available through LEO's hosted or portal services are the responsibility of the agency that owns the system (the system owner).

The FBI is responsible for any FBI owned systems that are accessible through LEO, and those systems will be scheduled under a separate disposition authority. The FBI, along with multiple other agencies, contributes content to LEO, and the contents of each system are the responsibility of the system owner. In the case of multi-agency inputs there may be joint or multi-party ownership of contributed data.

LEO's decentralized ownership and ownership responsibilities are communicated through various methods including: a content policy, the user application agreement, and online security messages.

A. SYSTEM DEVELOPMENT, OPERATIONS, AND MAINTENANCE RECORDS

1. System Documentation: Records relating to the design, implementation, testing, and validation of LEO including data system specifications, file specifications, concept of operations (CONOPS), systems security plan, codebooks, record layouts, user guides, output specifications, and final reports. Also included are records created or used to perform configuration/change management processes, including performance, capacity, and system management.

Disposition

DELETE/DESTROY records 1 year after termination of LEO.

2. Records (White Papers, Specifications, Proposed Modifications, etc.) for LEO Projects that are not implemented.

Disposition
DELETE/DESTROY 1 year after final decision is made. (GRS 24, Item 11a).

3. Installation and Testing Records.

Disposition
DELETE/DESTROY 3 years after final decision on acceptance is made (GRS 24, Item 11c).

4. Help Desk: These records are related to the customer services function and include logs, reports, and other files related to customer query and problem response; query monitoring and clearance; customer feedback; and related trend analysis and reporting.

Disposition
DELETE/DESTROY 1 year after record is superseded or obsolete or when no longer needed for review and analysis, whichever is later. (GRS 24, Items 10a&b).

5. Records Maintained by LEOSIG Moderators: For each LEOSIG, there are one or more employees, from one or more agencies, who serve as moderator(s) and are responsible for the administration of each LEOSIG's web content and access. To perform LEOSIG administration, moderators create and use records to communicate with members, LSU, and the PMO. Administrative records are also created or used relating to LEOSIG and Sub-SIG account(s) membership; available content and posting of content; web design; mail list and newsgroup issues and participation; and the calendar and address book functions.

Disposition
DELETE/DESTROY the moderators' records 1 year after termination of the corresponding LEOSIG.

6. Account Management System (AMS): Individuals requesting access to LEO and LEOSIGs complete a user application. Information from the application goes through a vetting or re-vetting process performed by PMO, the CJIS Division at Clarksburg, West Virginia, and the help desk at LSU. The process includes: data entry, data verification, approval/rejection, and account activation in the AMS.

The help desk and system administrators utilize the AMS to assist with user account and LEOSIG account maintenance. For the user accounts, information is entered into a user profile. Each LEOSIG also has a profile in AMS that contains information such as the LEOSIG's name and moderator name(s).

Electronic and hard copy statistical reports on user and LEOSIG accounts are generated from AMS. A dynamically updated address book comprised of information on LEO users, such as user names and e-mail addresses, is available to the user community.

Disposition
a. Approved applications and account data: DELETE/DESTROY approved applications and user account data 6 years after a user account is terminated or when no longer needed for investigative or security purposes, whichever is later. (GRS 24, Item 6a).

b. Rejected applications: DELETE/DESTROY rejected applications when 2 years old or when no longer needed for investigative or security purposes, whichever is later.

c. LEOSIG account data: DELETE/DESTROY LEOSIG account data 6 years after a LEOSIG account is terminated.

d. Statistical reports: DELETE/DESTROY statistical reports 6 years after the date of the report or when no longer required, whichever is later.

B. CONTENT RECORDS

LEOSIG moderators submit content to LSU via e-mail, facsimile, or standard mail. Once received, LSU prepares the content for posting, uploads onto the LEO web server, and updates LEO web pages that require links to the new content. LEO's content, which is accessible to users for viewing, printing or downloading, includes documents, spreadsheets, presentations, images, and other files.

Disposition

1. **a. Web Content ~~Contributed by the FBI~~** changed per FBI 3/17/06 SM

DELETE/DESTROY copy provided to LSU 60 days after successful posting of the content.

2. DELETE/DESTROY posted content when superseded or obsolete. [Consistent with the FBI Internet Web Site Records Disposition Authority (N1-065-04-6), content posted by the FBI will be covered by a records schedule developed for the FBI office/organization that originated the content.]

X ~~**b. Web Content Contributed by Other Agencies**~~ deleted per FBI 3/17/06 SM

~~Each contributing agency is responsible for developing disposition instructions for the content and communications posted on LEO by their employees.~~

C. RELATED RECORDS

1. Backups: Backups are maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

Disposition

DELETE/DESTROY incremental backups when superseded by a full backup or when 90 days old.

DELETE/DESTROY full backups when a more current full backup has been successfully captured or when 90 days old.

2. Security Audit Logs: LEO's Oracle databases capture database-specific events, including logins, accesses, and administrative activities. Logs are produced by different LEO applications to capture date, time, session statistics, and errors during user sessions. Detailed auditing is conducted to track which user modified which data element on a specific date and time. Automated security systems track audit information for activities, e.g. when a user is added or when a server is down.

Disposition

DELETE/DESTROY when 4 years old or when no longer needed for administrative, legal, audit, or other operational purposes, whichever is later.