U.S. Department of the Interior
DECOMMISSIONING PRIVACY THRESHOLD ANALYSIS

Introduction

The Department Privacy Office ensures that system decommissioning activities comply with current federal privacy regulations and standards, effectively mitigating risks associated with Personally Identifiable Information (PII) and maintaining comprehensive documentation. The Decommissioning Privacy Threshold Analysis (DPTA) aligns with federal privacy and security compliance requirements outlined in Section 208 of the E-Government Act of 2002, the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) Circular A-130, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, and NIST SP 800-37 Rev. 2.

This DPTA ensures that the retirement or transition of federal systems, applications, or services is conducted securely, preventing unauthorized access or disclosure of PII, ensuring adherence to National Archives and Records Administration (NARA) records retention schedules, and maintaining compliance with data sanitization requirements described in NIST SP 800-88, Guidelines for Media Sanitization. The analysis documented by this DPTA provides essential evidence of due diligence in meeting federal cybersecurity, privacy, and data disposition mandates throughout the decommissioning lifecycle. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PTA Guide.

Section 1: System Information

System Information

System: Incident Management Analysis and Reporting System
System Acronym: IMARS
Date submitted for review: February 3, 2026

System Manager

Name: Theresa Beazer
Title: ISSM
Bureau: Office of the Secretary
Phone: 720-298-0095
E-mail: theresa_beazer@ios.doi.gov

Information Systems Security Officer

Name: Omer Al-Samarae
Title: ISSO
Bureau: Office of the Secretary
Phone: 202-256-8859
E-mail: omer_al-samarae@ios.doi.gov

1. What was the purpose of the system?

IMARS was used to track law enforcement incidents and allowed sharing of incident or suspicious activity information with Federal agencies and other law enforcement organizations. IMARS, based on the NICHE Records Management System (RMS) developed by NICHE Technology, is a multi-tier, commercial-off-the-shelf (COTS) product providing incident management and reporting capabilities; however, the DOI needed updated technology.

Also, all sharing occurred in compliance with the routine uses described in its system of record notice, DOI-10, Incident Management, Analysis and Reporting System. All Memorandums of Understanding were also terminated, and no active data-sharing agreements remain in place with this legacy system.

2. Why is the system being decommissioned?

IMARS is being decommissioned as it has been succeeded by LE RMS, the department's modernized law enforcement records management system. The data in IMARS has been migrated to LE RMS.

3. What bureaus or offices were using this system?

Department Wide.

4. Was this system internally developed or a third-party service?

☐ Developed Internally
☒ Third-Party Service

5. Is this a cloud-based system?

☒ No
☐ Yes

6. List associated privacy compliance documentation, if applicable:

System of Record Notice(s): DOI-10, Incident Management, Analysis and Reporting System

Privacy Impact Assessment PIA(s): IMARS PIA 20251202

Section 2: PII & Data Disposition

1. Did the system contain, process, or transmit PII?

☐ No, Skip to Section 6.
☒ If yes, what type(s) of PII?

☒ Name (full, first or last)
☒ Aliases/nickname
☒ Driver's license
☒ Citizenship
☒ Legal Status
☒ Sex
☒ Race or ethnicity
☒ Date of birth
☒ Place of birth
☒ Home telephone number
☒ Personal Email
☒ Mailing or home address
☒ Religious preference
☒ Mother's maiden name
☒ Marital status
☒ Spouse Information
☒ Child or family information
☒ Emergency contact info
☒ Employment or resume info
☒ Full or Truncated SSN
☒ Physical characteristics
☒ Biometrics/facial recognition
☒ Vehicle information
☒ Passport information
☒ Travel information
☒ Parent's name
☒ Credit card number

☒ Personal cell phone number
☒ Tribal or other ID number
☒ Military records
☒ Financial information
☒ Education information
☒ Other: Describe below
☒ Nationality
☒ Disability Information

Law enforcement incident reports, law enforcement personnel records, law enforcement training records, images and videos collected from audio/visual recording devices such as surveillance cameras, closed circuit television located at DOI facilities for security and/or law enforcement operations, a mobile video recorder installed on a patrol vehicle and a wearable video recorder

2. What was the source of the PII?

☒ User-submitted (e.g., contact forms)
☐ Automatically collected (e.g., cookies, trackers)
☐ Derived analytics (e.g., engagement trends)
☐ Publicly visible profile data
☒ Other: *Specify below*

Federal, tribal, state and local agencies; Third-party sources

3. Did the system collect, process, or retain information on: (Please check all that apply)

☒ Federal Employees
☒ Contractors
☒ Members of the Public
☒ Volunteers
☐ Other (Describe)

4. How was PII used in the system? "(See latest approved PIA for details)"

System was used department wide by Law Enforcement officers for records of incidents and reports.

5. What is the NARA- approved schedule(s) for data in the system?

NARA General Records Schedule (GRS) 3.2, DAA-GRS2013-0006- 0003. All IMARS data has been migrated to the successor system, LE RMS. .

6. Have any unscheduled records been identified for data in the system? (if yes, describe the plan for scheduling or disposition)

N/A.

7. Has PII been transferred to another system or archived according to the records retention policy?

☒ Transferred to another system:
☐ Archived according to the records retention policy

Yes, IMARS has been migrated to the successor system, LE RMS. Data validation and integrity have been thoroughly tested, with 3 rounds of data migration validation.

8. If there are paper records associated with the system, please explain how the paper records will be

handled.

There are no paper records associated. All records are digitalized and migrated to the successor system.

9. If PII has been deleted, were NIST SP 800-88: Guidelines for Media Sanitization methods used?

☐ No: *Provide justification why and a timeline for completion*
☒ Yes

All data has been migrated to the successor system LE RMS, and OCIO hosting would perform proper Media Sanitization per NIST 800-88.

10. Were users notified about the data disposition or system decommissioning?

☐ No
☒ Yes

Section 3: System Dependencies & Third-Party Services

1. Does this system have any dependencies on other systems?

☒ No
☐ Yes

2. Are there any third-party service providers involved in system operations?

☒ No
☐ If yes, have contracts been reviewed for termination?

3. Were there any interconnections to external systems that required decommissioning?

☒ No
☐ Yes: *List the Connections and their decommissioning date*

4. If the system was cloud-based, has data been deleted per the cloud provider's policies?

☒ No
☐ Yes

5. Have all data-sharing agreements (DSAs) and Memorandums of Understanding (MOUs) been reviewed and terminated?

☐ No
☒ Yes

Section 4: Security & Compliance

1. Have all user accounts been disabled and access revoked?

☐ No: *Provide justification why and a timeline for completion*
☒ Yes

Yes, all IMARS users have been disabled and system shutdown. This was done to ensure no modifications occur on the legacy system as all the users have been migrated to the successor system LE RMS.

2. Has an exit security assessment been conducted by the ISSO?

☐ No
☒ Yes

3. Has a penetration test or vulnerability scan been conducted before decommissioning to identify residual risks?

☐ No
☒ Yes

4. Have all cryptographic keys and access credentials been securely deleted?

☐ No
☐ Yes
☒ N/A

5. Has an audit of the system's last active logs been conducted before decommissioning?

☐ No
☒ Yes

6. Have all audit logs, configurations, and system documentation been retained per NARA General Records Schedule (GRS) 3.2 – Information System Security Records?

☐ No
☒ Yes
☐ N/A

7. Briefly describe any privacy risks associated with the decommissioning of this system and how information will be handled (e.g., destroyed, archive, transferred, etc.). For each risk identified, please indicate how that risk will be mitigated. "See current approved PIA for insight"

All IMARS data has been migrated to the successor system, LE RMS.

Section 5: Final Approval

1. Who conducted the final review to confirm that all closure tasks, including data deletion and system/service retirement, were completed?

Information System Security Officer

2. Were all required stakeholders (Privacy, Security, Records Management, IT, System Owner, Risk Manager) involved in sign-off?

☐ No
☒ Yes

3. Who has been designated as the custodian of archived data?

Name: Omer Al-Samarae
Title: Information System Security Officer
Office: Office of Law Enforcement and Security
Phone: 202-256-8859
E-mail: omer_al-samarae@ios.doi.gov