# Department of the Interior
# Law Enforcement Policy

---

**Effective Date:** July 17, 2014
**Series:** Law Enforcement and Security
**Chapter 13:** Incident Management, Analysis, and Reporting System (IMARS)

**Originating Office:** Office of Law Enforcement and Security

13.1 **Purpose.** This chapter establishes standards for bureau/office law enforcement programs to operate the Incident Management, Analysis and Reporting System (IMARS). IMARS provides a Department-wide information collection, analysis, and reporting system for law enforcement incidents.

13.2 **Scope.** This policy applies to all law enforcement bureaus/offices of the Department of the Interior (Department / DOI).

13.3 **Authority.** This policy is issued pursuant to 112 DM 17 and 212 DM 17.

13.4 **Responsibilities.**

A. Deputy Assistant Secretary, Public Safety, Resource Protection, and Emergency Services (DAS-PRE) is the Executive Sponsor and Approving Official responsible for being the segment champion and initiating the business case for IMARS; controlling the overall funding and resources for the project; and providing the Authorization to Proceed (ATP) decision on key project phases.

B. Director, Office of Law Enforcement and Security (OLES) is the Executive Sponsor responsible for establishing and monitoring the business case and funding and providing leadership for IMARS policy development as well as program guidance and oversight of the Department's law enforcement programs.

C. Assistant Director, Law Enforcement Technology Division (LETD) is the IMARS System Owner responsible for making strategic decisions, approving budget and staffing levels, approving security/risk management strategies, and is ultimately responsible for all system problems or security compromises.

D. Law Enforcement Board of Advisors (BOA) consists of the Bureau/Office Director (or equivalent) of Law Enforcement (BDLE) of each program and is responsible for promulgating and complying with this policy.

E. Bureau Director of Law Enforcement (BDLE) is responsible for development and oversight of a bureau/office IMARS Standard Operating Procedures (SOP) manual. In addition, the BDLE is responsible for ensuring that any Department amendments are reflected in the bureau/office IMARS SOP manual and are communicated to the organization for immediate implementation.

F. IMARS Governance Council (IGC) provides voting representation for the stakeholder bureaus/offices and acts as the IMARS Change Control Board. The IGC consists of at least two members from each bureau/office with a law enforcement program; one law enforcement expert and one IT expert. The law enforcement representatives will ensure that IT is firmly based on the business needs of DOI and the bureaus/offices. The IT representatives will ensure that the IMARS solution architecture is compliant with bureau/office and Department enterprise architecture guidelines.

G. IMARS Change Control Board (CCB) is the committee that makes decisions regarding whether or not proposed changes to a software project should be implemented (see IGC).

H. Bureau/Office Deployment Managers (BDMs) ensure that each employee requesting access to IMARS has completed training and assists in getting IMARS installed, tested, and maintained on users' computers. BDMs define the process and timeline for roll-out of the IMARS program to bureau/office users based on Department guidance and in coordination with bureau/office IT, training, and operations programs. BDMs request user accounts, VPN access and installation packages and updates. They also provide first level support (or leverage existing IT support environments) to users as appropriate. Each bureau/office with a law enforcement program has at least one deployment manager or team of deployment managers.

I. Law Enforcement Technology Division (LETD) IMARS Support Group is a group of individuals that provide business and technical support to all BDMs and sometimes, individual IMARS users. They track and coordinate change requests and service tickets, troubleshoot, and escalate to other IT support elements or contractors as appropriate.

13.5 **Policy.** This chapter establishes policy and standards for the implementation and use of the IMARS. Bureaus/offices must develop Standard Operating Procedures (SOPs) that provide specific guidance in the areas of implementation, operations, records management, access, and security to meet the following guidelines:

A. Implementation.

(1) Identify IGC representatives and BDMs.

(2) Implement IMARS throughout bureau/office law enforcement and security programs.

(3) Establish and implement IMARS training and deployment SOPs.

(a) All employees must receive a minimum of eight hours training prior to being authorized access and utilize IMARS.

(b) When available, it is recommended IMARS training be conducted in a face-to-face training environment. Bureaus/offices may use other training methods that are approved by the BDM.

(4) Ensure program users are provided appropriate hardware and network connectivity to access the IMARS application.

(5) Ensure appropriate funding is allocated for the implementation and operation of the IMARS system within the bureau.

B. Operations.

(1) Ensure that bureaus/offices respond to the mandatory reporting elements in IMARS as required by the Department and OLES as established in related law enforcement policies.

(2) Report bureau-level statistics for use in the National Incident-Based Reporting System (NIBRS). IMARS will comply with the Uniform Crime Reporting Act of 1988 and will serve as the primary Law Enforcement System of Record and DOI reporting conduit to NIBRS.

(3) Report suspicious activities in IMARS in accordance with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). IMARS will provide SAR reporting in an initiative to provide law enforcement with another tool to help prevent terrorism and other related criminal activity. IMARS will be the primary Department reporting conduit to the Department of Justice (DOJ) and Department of Homeland Security (DHS) by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

C. Records Management.

(1) Publish internal guidelines regarding the creation and maintenance of law

enforcement records that are not in conflict with IMARS records management policies and procedures. IMARS records management policies and procedures are established to support bureau/office policies and are not intended to dictate practices in individual offices.

(2) Maintain information in a manner that is secure yet allows for effective storage, retrieval, cross-referencing, and analysis.

(3) General and specific information obtained from IMARS may only be used for official law enforcement purposes and will not be released to any unauthorized person.

(a) Verbal and written reports are to be handled in accordance with current Controlled Unclassified Information (CUI) procedures and appropriate designations, such as For Official Use Only (FOUO) and Law Enforcement Sensitive markings.

(b) Any printed and/or viewed information from another agency or domain within or through IMARS may not be disclosed publicly without the consent of the agency or domain that originated the data and in accordance with the Freedom of Information Act (FOIA) regulations.

(c) All documents produced from IMARS which are no longer active, will be destroyed according to applicable retention and destruction schedules.

(d) Bureaus/offices must ensure that there is a periodic review and evaluation to assure that information being utilized in their IMARS domain is appropriate and data collected and stored is both necessary and sufficient.

(e) Bureaus/offices must ensure that records created and maintained in law enforcement collection systems meet the National Archives and Records Administration Record Schedules, the IMARS approved Record Schedule, and all appropriate laws and regulations, including FOIA, Privacy Act, and Federal Records Act.

D. Access/Security.

(1) Bureaus/offices must administer the program to ensure strict adherence to all security requirements according to the IMARS System of Record Notice (SORN) and as directed by the DOI Office of the Chief Information Officer (OCIO) in order to ensure:

(a) IMARS resources are used only by authorized personnel.

(b) Employees will comply with security measures built into IMARS software per National Institute of Standards and Technology information security standard NIST 800-53 to include the use of domain identification, user identification, password identification, and role restrictions.

(c) Employee roles and the access appropriate for each employee user of IMARS will be defined. Employees will only receive roles suitable to the duties they are required to perform.

(d) Employees receive adequate training so that they may fulfill their information technology security responsibilities (375 DM 19.5(D)).

(e) Suspected, actual, or threatened information technology security incidents will be immediately reported to the proper authorities.

(f) Failure to adhere to federal and Department regulations pertaining to IMARS and other information technology resources will result in appropriate administrative, disciplinary, or legal action being taken against the violator (375 DM 19.5(E)).

(g) BDLEs and each user are responsible for the overall integrity, confidentiality, and security of their IMARS program.

(h) A BDLE or the Director, OLES may access IMARS data or system reports that fall within their scope of responsibility due to operational or administrative necessity, or to respond to inquiries under the FOIA and/or the Protection of Privacy Act.

(i) Information, data, or reports will be shared equally and made available across all DOI bureaus/offices. Bureaus/offices may restrict sensitive or need to know information based on the circumstances of the incident. However, in general, all basic information entered into IMARS will be available for viewing by all DOI authorized personnel.

(j) Users are responsible for special protection and security of sensitive data, e.g., juvenile records, internal affairs records, etc.

(k) Information will be available to the public under the guidance of the System of Record Notice per the Privacy Act of 1974.

(l) Public requests for information should be directed to the bureau/office FOIA officer.