

Department of the Interior
Privacy Impact Assessment Template

March 8, 2013

Name of Project: Incident Management Analysis and Reporting System

Bureau: Office of the Secretary

Project's Unique ID: 010-000-03-00-02-0020-00

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

A. CONTACT INFORMATION:

Departmental Privacy Office
Office of the Chief Information Officer
U.S. Department of the Interior
202-208-1605
DOI_Privacy@ios.doi.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) **Does this system contain any information about individuals?**

Yes, the IMARS system contains the following personal information about individuals:

- SSN
- Name
- Home address
- Work address
- Phone numbers
- Emergency contact information
- Ethnicity and race
- Driver's license or non-driver's identification number
- Date of birth
- Gender
- Physical description of the individual including any and all physical attributes (may include photos and videos)
- Incident data (criminal activity, response, outcome of incident, etc)

a. Is this information identifiable to the individual¹?

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes, many of the data types listed above are identifiable to the individual, either alone or in combination with other data types.

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes, the IMARS system contains data about individual members of the public who are involved in incidents entered into the IMARS system.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, the system includes information about DOI law enforcement personnel and other employees who are users of IMARS.

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

2) What is the purpose of the system/application?

IMARS is an incident management and reporting commercial-off-the-shelf (COTS) product which will enhance the following abilities:

- Prevent, detect and investigate known and suspected criminal activity.
- Protect natural and cultural resources.
- Capture, integrate and share law enforcement and related information and observations from other sources.
- Identify needs (training, resources, etc.).
- Measure performance of law enforcement programs and management of emergency incidents.
- Meet reporting requirements including, DOI Level 1 and Level 2 Significant Incidents, and Department of Homeland Security (DHS) and National Incident Based Reporting System (NIBRS). Interface frameworks (interfaces will be implemented in future releases of IMARS).
- Analyze and prioritize protection efforts.
- Justify requests and expenditures.
- Assist in managing visitor use and protection programs.
- Training (including incorporating into Federal Law Enforcement Training Center (FLETC) programs)
- Investigate, detain and apprehend those committing crimes on DOI lands.
- Investigate and prevent visitor accidents and injuries on DOI lands.

3) What legal authority authorizes the purchase or development of this system/application?

Public Law 100-690 -Uniform Federal Crime Reporting Act; Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (pub. L No. 108-458); Departmental Manual 446, Law Enforcement, Chapter 15, Records System

C. DATA in the SYSTEM:

1. What categories of individuals are covered in the system?

The categories of individuals covered in the system include IMARS system users and DOI law enforcement personnel, including current and former Federal employees and contractors, as well as tribal, state and local law enforcement officers. Additionally, this system contains information on members of the general public, including individuals or groups of individuals involved with law enforcement incidents concerning Federal assets or

occurring on public lands and tribal reservations or adjacent lands under concurrent jurisdiction, such as witnesses, victims, individuals making complaints, individuals being investigated or arrested for criminal or traffic offenses, or certain types of non-criminal incidents; and members of the general public involved in an accident on DOI managed properties or tribal reservations.

2. What are the sources of the information in the system?

Sources of information in the system include Department, Bureau, office, tribal, state and local law officials and management, complainants, informants, suspects, victims, and witnesses.

The Federal Bureau of Investigation (FBI) and the Department of Justice, as well as other federal law enforcement, corrections and homeland security agencies may also serve as sources of information for the system. DOI Internal Affairs may append additional information to a case file when conducting their own investigations and other federal law enforcement, corrections and homeland security agencies may serve as sources of information for the system.

Data will primarily be added by DOI law enforcement agents during law enforcement investigations. In the future, this will include the automated addition of data from third party Computer Aided Dispatch (CAD) interfaces with IMARS, including software from CrimeStar, CIS, Motorola, and Logysis. The data flow from CAD interfaces will be unidirectional, with data fed in an XML format from the CAD system to IMARS.

In addition, data may be obtained from existing DOI Bureau law enforcement offices that are transitioning from their own law enforcement management information systems to IMARS. The transitioning Bureaus are:

- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- Bureau of Reclamation (BOR)
- Fish and Wildlife Service (FWS)
- National Park Service (NPS)
- U.S. Park Police (USPP)

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Some information is received from individuals, such as complainants, informants, suspects, victims, witnesses and law enforcement officials. Other sources include DOI or bureau law enforcement offices, officials

and management, as well the FBI, the Department of Justice, and tribal, state and local law agencies.

b. What Federal agencies are providing data for use in the system?

The FBI, Department of Justice, and other Federal law enforcement agencies may provide data for use in the system.

c. What Tribal, State and local agencies are providing data for use in the system?

Tribal, state and local law enforcement, corrections and security agencies could provide incident related data to be included in IMARS.

d. From what other third party sources will data be collected?

Data may be collected from a variety of other sources, including but not limited to telephone, text message or email records obtained from cellular carriers, internet service providers, and others. In addition, information may be obtained from public access web sites, newspapers, press releases, or other similar sources.

e. What information will be collected from the employee and the public?

Incident and non-incident data related to criminal and non-criminal activity will be collected for the department supporting law enforcement, homeland security, and security (physical, personnel and stability, information, and industrial). This may include data documenting investigation activities, traffic safety, or domestic issues. Data relating to emergency management, sharing and analysis activities of the department will also be collected.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

The system provides for a variety of data validation checks to ensure that the proper data types are entered into certain data fields. The individual collecting the data and entering the data into IMARS will verify the accuracy of data collected pursuant to policy and procedures defined by each agency that uses IMARS. Supervisors will also review data for accuracy as well.

b. How will data be checked for completeness?

The system provides for a variety of data validation checks to ensure that complete entries are provided in certain data fields. The individual collecting the data and entering the data into IMARS will verify the completeness of the data collected pursuant to policy and procedures defined by each agency that uses IMARS. Supervisors will also review data for completeness as well.

- c. Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Pursuant to policies and procedures defined by the agencies that use IMARS, system users and supervisors are responsible for ensuring the data in IMARS remains current.

- d. Are the data elements described in detail and documented?** If yes, what is the name of the document?

The IMARS data elements are described in the Data Element Report-Law Enforcement View Data Dictionary. Access to the dictionary is provided by the IMARS Program Office.

D. ATTRIBUTES OF THE DATA:

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes, the system is designed as a law enforcement records system, and the data is both relevant and necessary to the purpose for which the system has been designed.

- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Yes, the system may derive new data or create previously unavailable data about an individual through data aggregation. The intent of the IMARS system is to serve as a law enforcement tool that will store data from the Department of the Interior's various law enforcement agencies. IMARS will also include data provided by other Federal, state, local, and tribal entities. Information obtained about specific individuals from various sources may be combined to create new data.

- 3) Will the new data be placed in the individual's record?**

The new data may be placed in individuals' records in the IMARS system or accessible through various searches or reports that are generated by the system. The new data may be used in the course of investigations or other law enforcement actions.

4) Can the system make determinations about employees/public that would not be possible without the new data?

Yes, the system may potentially be used to make decisions about individuals that would not be possible without the new data. In particular, the data may be used to make determinations related to criminal investigations.

5) How will the new data be verified for relevance and accuracy?

The new data would be verified for accuracy through the use of data intelligence analysis tools, research, investigation techniques and review by IMARS users and supervisors.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

IMARS utilizes a variety of system access and security controls, as defined in the system security plan (SSP), including limited system access through logical and physical controls.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Not applicable – processes are not being consolidated.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved using a variety of personal identifiers, either individually or in combination, including:

- Social Security Number
- Name
- Driver's license or non-driver identification number
- Home address
- Work address
- Phone numbers
- Emergency contact information
- Ethnicity and race
- Date of birth

- Gender
- Physical description of the individual including any and all physical attributes (may include photos and videos)
- Incident data (criminal activity, response, outcome of incident, etc)

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Summary and detailed reports can be produced on individuals. These reports may be used for court cases, assisting with an investigation, intelligence gathering, all in the furtherance of the law enforcement process. Reports are available to any authorized user. A user's level of authorization is based on the group role or roles assigned to the individual.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Individual members of the public have the opportunity or right to decline to provide information where providing information is voluntary. Individuals will be informed of this right by the law enforcement officer requesting the information.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

IMARS is hosted at one site.

2) What are the retention periods of data in this system?

Records in this system are retained and disposed of in accordance with Office of the Secretary Records Schedule 8151, Incident, Management, Analysis and Reporting System, which was approved by the National Archives and Records Administration (NARA) (N1-048-09-5), and other NARA approved bureau or office records schedules. The specific record schedule for each type of record or form is dependent on the subject matter and records series.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

After the retention period has passed, temporary records are disposed of in accordance with the applicable records schedule and DOI policy. Disposition

methods include burning, pulping, shredding, erasing and degaussing in accordance with DOI 384 Departmental Manual 1. Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA guidelines. The procedures are documented in the IMARS Records Schedule cited above.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

The IMARS system will use one type of new technology that has not been used by prior DOI law enforcement systems. One source of data for the system will be the automated addition of data from third party Computer Aided Dispatch (CAD) interfaces with IMARS, including software from CrimeStar, CIS, Motorola, and Logisys. The data flow from CAD interfaces will be unidirectional, with data fed in an XML format from the CAD system to IMARS.

5) How does the use of this technology affect public/employee privacy?

This CAD interfaces will facilitate the entry of law enforcement dispatch communications into IMARS. Previously, relevant dispatch information was entered manually into DOI's law enforcement records systems. The computer aided dispatch interfaces will ease the process of data entry and are likely to reduce data entry errors. The use of the CAD interfaces is not expected to have a negative effect on public or employee privacy.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

IMARS does not provide for active, real time monitoring. However, individuals can be monitored to the extent that the system includes ongoing data such as reported location sightings or credit card or telephone records.

The system provides users with the capability to identify and locate individuals using data contained in the system, including physical attributes of an individual (including text, photos, and video), personal and professional physical addresses, and personal and professional phone numbers.

IMARS has an audit log that can be used to run reports on individual users' access to and actions within the system. Additionally, IMARS contains a user traceability program that can detect unauthorized access attempts or access to files outside of an authorized user's permissions.

7) What kinds of information are collected as a function of the monitoring of individuals?

While the data in the system can be used to perform limited types of monitoring, as described in the previous paragraph, the system does not actively monitor individuals and new information is not collected or derived through monitoring activities.

8) What controls will be used to prevent unauthorized monitoring?

The confidentiality of user sessions over the intranet is maintained through the use of secure connections. In addition, a network intrusion detection system, and firewalls are used to prevent unauthorized monitoring:

Only authorized users who have been given a username and password will be able to access the system. In addition, all users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter. The system's audit trail feature, unique identification, authentication and password requirements, along with mandatory security, privacy and records management training requirements, help prevent unauthorized monitoring, as well as unauthorized access to data, browsing and misuse. In addition, IMARS provides the ability to minimize all windows with a single click to reduce the opportunity for non-users to view system information.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Incident Management, Analysis and Reporting System, DOI-10. Anticipated publication of this new system of records notice is anticipated early in 2013.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

As discussed above, a new system of records notice is being developed.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Trained and authorized Federal employees, contractors, managers, program office and system administrators, and tribal law enforcement personnel will have access to the data in IMARS.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Requests for access for a particular user are initiated by authorized personnel at each Bureau law enforcement office. A Bureau Representative will evaluate the request and follow procedures to determine and grant individuals access to the data. Least privileges determine that only the minimum levels of access required to perform job functions are granted to users.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

No, access to records in the system is limited to authorized personnel on an official "need to know" basis. Electronic data is protected through user identification, passwords, database permissions and software controls. Such security measures establish different access levels for different types of users associated with pre-defined groups at each of the Bureaus utilizing IMARS. Each user's access is restricted to only the functions and data necessary to perform job responsibilities. Access can be restricted to specific functions (create, update, delete, view, assign permissions) and is restricted utilizing role-based accounts.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Access granted to individuals is password-protected; each person granted access to the system must be trained and individually authorized to use the system. Each user is assigned to roles which grant access to specific data within the system. IMARS logs events including user login/logout, searches, views, printing, and data alterations. These events are reviewed by system administrators on a regular scheduled basis. All users must accept and consent to established rules of behavior before accessing the system and follow established internal security protocols.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors have been involved in the design, development and maintenance of the system, and Privacy Act clauses were included in their contracts.

6) Do other systems share data or have access to the data in the system? If yes, explain.

Except as described elsewhere in this PIA, other systems do not share data or have access to the data in IMARS.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The system manager, security manager and system administrator for IMARS will have the responsibility for protecting the privacy rights of the public and employees.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

Other agencies do not share data or have direct access to IMARS but other federal, state, local, and other law enforcement agencies will have data reported and shared to them based on current regulations and through joint law enforcement operations.

9) How will the data be used by the other agency?

Data may be directly used for crime statistics reporting, criminal investigations and apprehension of criminals or suspected criminals, identification or location of missing persons, identification or location of property and/or evidence, and public safety awareness. Data may also be used in criminal or non-criminal analysis to provide statistical data that will enhance law enforcement, security, or safety decisions.

10) Who is responsible for assuring proper use of the data?

The IMARS System Owner and System Manager will be responsible for assuring proper use of the data. All Federal employees with authorized access are responsible for assuring proper use of the data, and must comply with the requirements in OMB Circulars A-123 and A130, Department of the Interior Departmental Manual 383 OM 3 (Privacy Act -Bureau Responsibilities), as well as the Rules of Behavior agreement.