[4310-RK-P]

DEPARTMENT OF THE INTERIOR

Office of the Secretary

XXXD4523WT DWT000000.000000 DS65101000

Privacy Act of 1974, as Amended; Notice of a New System of Records

AGENCY: Department of the Interior.

ACTION: Notice of Creation of a New System of Records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a), the Department of the Interior is issuing a public notice of its intent to create the Office of the Secretary Incident Management, Analysis and Reporting System system of records. The Incident Management, Analysis and Reporting System will provide a unified system for Department of the Interior law enforcement agencies to manage law enforcement investigations, measure performance and meet reporting requirements. The Incident Management, Analysis and Reporting System will incorporate current Department of the Interior law enforcement systems utilized by the Bureaus. This newly established system will be included in the Department of the Interior's inventory of record systems.

DATE: Comments must be received by [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER.]. This new system will be effective [INSERT DATE 40 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Any person interested in commenting on this amendment may do so by: submitting comments in writing to the OS/IBC Privacy Act Officer, 1849 C Street N.W., Mail Stop 2650 MIB, Washington, D.C. 20240; hand-delivering comments to the

OS/IBC Privacy Act Officer, 1849 C Street N.W., Mail Stop 2650 MIB, Washington, D.C. 20240 or e-mailing comments to *privacy@nbc.gov*.

FOR FURTHER INFORMATION CONTACT: System Manager - IMARS, 13461 Sunrise Valley Drive, Herndon, VA 20171, or by phone at 703-793-5091.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of the Interior (DOI), Office of the Secretary, has created an enterprise-wide system, known as the Incident Management, Analysis and Reporting System (IMARS) system of records, to consolidate law enforcement incident management and reporting among the various Bureaus and Offices with law enforcement duties within DOI. IMARS will improve the following capabilities of the Department: 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); measure the performance of law enforcement programs and operations; meet reporting requirements; provide the capability to interface with Department of Homeland Security and National Incident Based Reporting System; analyze and prioritize protection efforts; provide information to justify law enforcement funding requests and expenditures; assist in managing visitor use and protection programs, including training; investigate, detain and apprehend those committing crimes on DOI properties or tribal reservations (for the purpose of this system of records notice, tribal reservations include contiguous areas policed by tribal or Bureau of Indian Affairs law enforcement offices) managed by a Native American tribe under DOI's Bureau of Indian Affairs; and investigate and prevent

visitor accident injuries on DOI properties or tribal reservations.

Incident and non-incident data related to criminal and civil activity will be collected in support of law enforcement, homeland security, and security (physical, personnel and stability, information, and industrial) activities. This may include data documenting investigations and law enforcement activities, traffic safety, traffic accidents and domestic issues, and emergency management, sharing and analysis activities.

In accordance with the Privacy Act of 1974, as amended, DOI proposes to consolidate the following DOI Privacy Act systems of records: Bureau of Reclamation Law Enforcement Management Information System (RLEMIS) – Interior, WBR-50 (73 FR 62314, October 20, 2008); Fish and Wildlife Service Investigative Case File System – Interior, FWS-20 (48 FR 54719, December 6, 1983); Bureau of Land Management Criminal Case Investigation – Interior, BLM-18 (73 FR 17376, April 1, 2008); Bureau of Indian Affairs Law Enforcement Services – Interior, BIA-18 (70 FR 1264, January 6, 2005); and National Park Service Case Incident Reporting System, NPS–19 (70 FR 1274, January 6, 2005) into one Department of the Interior system of records, titled the Incident Management, Analysis and Reporting System (IMARS). The consolidated system will be maintained by DOI's Office of Law Enforcement Services. The system will be managed by the IMARS Security Manager (the "System Manager").

In a notice of proposed rulemaking, which is published separately in the Federal Register, the Office of the Secretary is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and

(k)(2). The exemptions for the consolidated system of records will continue to be applicable until the final rule has been completed.

The system will be effective as proposed at the end of the comment period (the comment period will end 40 days after the publication of this notice in the Federal Register), unless comments are received which would require a contrary determination. DOI will publish a revised notice if changes are made based upon a review of the comments received.

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal Agencies collect, maintain, use, and disseminate individuals' personal information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particulars assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. As a matter of policy, DOI extends administrative Privacy Act protections to all individuals. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations, 43 CFR part 2.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains and the routine uses of each system to make agency recordkeeping practices transparent, notify individuals regarding the uses of their records, and assist individuals to

more easily find such records within the agency. Below is the description of the Office of the Secretary Incident Management, Analysis and Reporting System (IMARS) system of records.

In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Disclosure

Before including your address, phone number, e-mail address, or other personal identifying information in your comment, you should be aware that your entire comment – including your personal identifying information – may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Date: July 18, 2013.

Signed: _____

David Alspach
OS/IBC Privacy Act Officer

SYSTEM NAME:

Incident Management, Analysis and Reporting System, DOI-10

SYSTEM LOCATION

Interior Business Center, U.S. Department of Interior, 7301 W Mansfield Ave, Denver, CO 80235.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered in the system include current and former

Federal employees and contractors, Federal, tribal, state and local law enforcement officers. Additionally, this system contains information on members of the general public, including individuals and/or groups of individuals involved with law enforcement incidents involving Federal assets or occurring on public lands and tribal reservations, such as witnesses, 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 properties or tribal reservations.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes law enforcement incident reports, law enforcement personnel records, and law enforcement training records, which contain the following information: Social Security numbers, drivers license numbers, vehicle identification numbers, license plate numbers, names, home addresses, work addresses, phone numbers, email addresses and other contact information, emergency contact information, ethnicity and race, tribal identification numbers or other tribal enrollment data, work history, educational history, affiliations, and other related data, dates of birth, places of birth, passport numbers, gender, fingerprints, hair and eye color, and any other physical or distinguishing attributes of an individual. Incident reports and records may include attachments such as photos, video, sketches, medical reports, and email and text messages. Incident reports may also include information concerning criminal activity, response, and outcome of the incident. Records in this system also include information concerning Federal civilian employees and contractors, Federal, tribal, state and local law enforcement officers and may contain information regarding an officer's name, contact information, station and

career history, firearms qualifications, medical history, background investigation and status, date of birth and Social Security Number. Information regarding Officers' equipment, such as firearms, tasers, body armor, vehicles, computers and special equipment related skills is also included in this system.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Uniform Federal Crime Reporting Act, 28 U.S.C. 534; Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458); Homeland Security Act of 2002 (Pub. L. 107-296); USA PATRIOT ACT of 2001 (Pub. L. No. 107-56); USA PATRIOT Improvement Act of 2005 (Pub. L. No. 109-177); Tribal Law and Order Act of 2010 (Pub. L. No. 111-211); Homeland Security Presidential Directive 7 - Critical Infrastructure Identification, Prioritization, and Protection; Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors; Criminal Intelligence Systems Operating Policies, 28 CFR part 23.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The primary use of the records is for an incident management and reporting application that 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; measure performance of law enforcement programs and management of emergency incidents; meet reporting requirements, provide Department of Homeland Security (DHS) and National Incident Based Reporting System (NIBRS) interface

frameworks; analyze and prioritize protection efforts; assist in managing visitor use and protection programs; employee training; enable the ability to investigate, detain and apprehend those committing crimes on DOI properties or tribal reservations; and to investigate and prevent visitor accident injuries on DOI properties or tribal reservations. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) (a) To any of the following entities or individuals, when the circumstances set forth in paragraph (b) are met:

(i) The U.S. Department of Justice (DOJ);

(ii) A court or an adjudicative or other administrative body;

(iii) A party in litigation before a court or an adjudicative or other administrative body; or

(iv) Any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;

(b) When:

(i) One of the following is a party to the proceeding or has an interest in the proceeding:

(A) DOI or any component of DOI;

(B) Any other Federal agency appearing before the Office of Hearings and Appeals;

(C) Any DOI employee acting in his or her official capacity;

(D) Any DOI employee acting in his or her individual capacity if DOI or DOJ

has agreed to represent that employee or pay for private representation of the employee;

(E) The United States, when DOJ determines that DOI is likely to be affected by the proceeding; and

(ii) DOI deems the disclosure to be:

(A) Relevant and necessary to the proceeding; and

(B) Compatible with the purpose for which the records were compiled.

(2) To a congressional office in response to a written inquiry that an individual covered by the system, or the heir of such individual if the covered individual is deceased, has made to the office, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(3) To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible for which the records are collected or maintained, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(4) To any criminal, civil, or regulatory law enforcement authority (whether Federal, State, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

(5) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(6) To Federal, State, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

(7) To representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

(8) To State and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

(9) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

(10) To appropriate agencies, entities, and persons when:

(a) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; and

(b) The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(c) The disclosure is made to such agencies, entities and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(11) To the Office of Management and Budget during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

(12) To the Department of the Treasury to recover debts owed to the United States.

(13) To a consumer reporting agency if the disclosure requirements of the Debt Collection Act, as outlined at 31 U.S.C. 3711(e)(1), have been met.

(14) To the Department of Justice, the Department of Homeland Security, and other federal, state and local law enforcement agencies for the purpose of information exchange on law enforcement activity.

(15) To agency contractors, grantees, or volunteers for DOI or other Federal Departments who have been engaged to assist the Government in the performance of a contract, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity.

(16) To any of the following entities or individuals, for the purpose of providing information on traffic accidents, personal injuries, or the loss or damage of property:

(a) Individuals involved in such incidents;

(b) Persons injured in such incidents;

(c) Owners of property damaged, lost or stolen in such incidents; and/or

(d) These individuals' duly verified insurance companies, personal

representatives, and/or attorneys.

(17) To any criminal, civil, or regulatory authority (whether Federal, State, territorial, local, tribal or foreign) for the purpose of providing background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

(18) To the news media and the public, with the approval of the System Manager in consultation with the Office of the Solicitor and the Senior Agency Official for Privacy, in support of the law enforcement activities, including obtaining public assistance with identifying and locating criminal suspects and lost or missing individuals, and providing the public with alerts about dangerous individuals.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic records are maintained in password protected removable drives and other user-authenticated, password-protected systems that are compliant with the Federal Information Security Management Act. All records are accessed only by authorized personnel who have a need to access the records in the performance of their official duties. Paper records are contained in file folders stored in file cabinets.

RETRIEVABILITY:

Multiple fields allow retrieval of individual record information including Social Security number, first or last name, badge number, address, phone number, vehicle information and physical attributes.

SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security rules and policies. During normal hours of operation, paper records are maintained in locked filed cabinets under the control of authorized personnel. Computerized records systems follow the National Institute of Standards and Technology standards as developed to comply with the Privacy Act of 1974 (Pub. L. 93–579), Paperwork Reduction Act of 1995 (Pub. L. 104–13), Federal Information Security Management Act of 2002 (Pub. L. 107–347), and the Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems. Computer servers in which electronic records are stored are located in secured Department of the Interior facilities.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties. 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 and/or bureaus. Each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. Access can be restricted to specific functions (create, update, delete, view, assign permissions) and is restricted utilizing role-based access.

Authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the Rules of Behavior. Contract employees with access to the system are monitored

by their Contracting Officer's Technical Representative and the agency Security Manager.

RETENTION AND DISPOSAL:

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. 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.

SYSTEM MANAGER AND ADDRESS:

IMARS Security Manager, 13461 Sunrise Valley Drive, Herndon, VA 20171.

NOTIFICATION PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the notification procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

RECORDS ACCESS PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the access procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request should describe the records sought as specifically as possible. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORDS PROCEDURES:

The Department of the Interior is proposing to exempt portions of this system from the amendment procedures of the Privacy Act pursuant to sections (j)(2) and (k)(2). An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the System Manager identified above. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

RECORD SOURCE CATEGORIES:

Sources of information in the system include Department, bureau, office, tribal, State and local law officials and management, complainants, informants, suspects, victims, witnesses, visitors to Federal properties, and other Federal agencies including the Federal Bureau of Investigation or the Department of Justice.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Privacy Act (5 U.S.C. 552a(j)(2) and (k)(2)) provides general exemption authority for some Privacy Act systems. In accordance with that authority, the Department of the Interior adopted regulations 43 CFR 2.254(a-b). Pursuant to 5 U.S.C.

552a(j)(2) and (k)(2) of the Privacy Act, portions of this systems are exempt from the following subsections of the Privacy Act (as found in 5 U.S.C. 552a); (c)(3), (c)(4), (d), (e)(1) through (e)(3), (e)(4)(G) through (e)(4)(I), (e)(5), (e)(8), (f), and (g).

[FR Doc. 2013-18224 Filed 07/29/2013 at 8:45 am; Publication Date: 07/30/2013]