U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Administrative and Law Enforcement Resource Management System (ALERMS)
Date: November 3, 2022
Bureau/Office: Bureau of Land Management, Arizona State Office, Mission Support Branch
Bureau/Office Contact Title: Associate Privacy Officer
Point of Contact
Name: Catherine Brean
Title: Associate Privacy Officer
Email: blm_wo_privacy@blm.gov
Phone: (830) 225-3459
Address: BLM, IRM, DOI National Operations Center, Bldg. 50, Denver, Colorado 80224

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Bureau of Land Management (BLM), Arizona State Office, Administrative and Law Enforcement Resource Management System (ALERMS) supports critical communication and resource tracking services for administrative and law enforcement employees within the Department of the Interior (DOI) and U.S. Department of Agriculture (USDA). The system

includes a commercial-off-the-shelf computer aided dispatch (CAD) system for event creation and management, integration with criminal justice information systems, and audio recording systems for mission critical radio and telephone communications.

The system includes:

- Creation and management of law enforcement field events including event location, involved persons and vehicles, associated property, and other information associated with carrying out law enforcement duties.
- Querying criminal justice information systems for information on involved persons and vehicles and associated property related to law enforcement events.
- Querying criminal justice information systems for the purposes of suitability and employment background investigations.
- Querying criminal justice information systems for law enforcement investigations.
- Creation and management of administrative field events such as search and rescue, daily field operations, and critical incidents occurring on public lands or involving employees supporting public lands.
- Record and retain mission critical radio and telephone communications associated with the Mission Support Communication Center.
- Tracking locations of law enforcement and administrative personnel while in the field for employee safety and support.

The ALERMS may use mobile applications integrated with the CAD system to allow law enforcement officers to perform event management and criminal justice functions while in the field. Functions performed from the field will be limited in scope and compliant with Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Security Policy.

C. What is the legal authority?

The legal authorities that authorize the collection and maintenance of this system of record are:

- Criminal Justice Information Systems 28 C.F.R. § 20;
- Department of the Interior DM Part 446, Chapter 14;
- Records maintained on individuals 5 U.S.C. 552a (j) (2);
- 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;Service First Authority (Public Law 113-76, Section 430 of the Consolidated Appropriation Act of 2014)

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes:

The ALERMS System Security and Privacy Plan (SSP) is under development and will be completed as part of the security assessment and authorization process to obtain an Authority to Operate (ATO) this system. The UII Code is 010-000002657.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Computer Information Systems (CIS) Computer Aided Dispatch (CAD) Server Applications	CIS CAD server applications manage interfaces, connections between subsystems, and user access for the system.	Yes	CIS CAD Server Applications do not retain any PII data, however, the applications are responsible for handling data exchanges between subsystems within the ALERMS, which may contain PII.
CIS CAD Desktop Application	CIS CAD desktop application is used by authorized users to create, manage, and view events within the system. Data entry includes all information associated with event management including location, involved persons and vehicles,	Yes	The CIS CAD desktop application allows the user to enter and retrieve data, which may contain PII, from specific government furnished and managed computers.

	associated property, and other event data. All data created and retrieved in CIS CAD desktop application is stored in the ALERMS SQL database. Only authorized users can access CIS CAD desktop application.		
Microsoft SQL Database	SQL database is used to store all event data supporting the CIS CAD application. This data includes event location, involved persons and vehicles, associated property, and other event data. SQL database also maintains authorized user access information and permissions for the CIS CAD application.	Yes	The SQL database stores all event data entered into the CIS CAD application including PII data.
Eventide NexLog Recorder	Eventide NexLog recorder is used for recording all mission critical voice communications including radio and telephone communications.	Yes	Recordings captured include routine radio transmissions and telephone calls including event information. The event information contained in audio recordings will include PII associated with law enforcement events.
ESRI ArcGIS Server	Provides base map and layers for use and integration with the CIS CAD application.	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: The records in this system are covered under the DOI-10, Incident Management, Analysis and Reporting System, 79 FR 31974 (June 3, 2014), modification published 86 FR 50156 (September 7, 2021), which can be found at https://www.doi.gov/privacy/doi-notices.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes:

☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: License Plate Numbers; Vehicle Identification Number; Boat Registration/Hull Number; Passport Numbers; Alien Registration Numbers; FBI Universal Control Numbers (UCN); State Identification Numbers (SID); Work Addresses; Other Contact Information; Tribal Enrollment Data; Work History; Educational History; Fingerprints; Hair and Eye Color and any other Physical or Distinguishing Attributes of an Individual; Arrest and incarceration records; Prior Contacts with Law Enforcement; Criminal History Record Information (CHRI); Photographs; Audio Recordings; Video Recordings.

Individual names, usernames, passwords, email addresses, phone numbers and Single-Sign On (SSO) information is collected as part of the system account management process. Username and password are required to access the application and is limited to authorized BLM employees with granular permissions based on job function.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency

☒ Tribal agency
☒ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems

The ALERMS receives criminal justice information through the Arizona Criminal Justice Information System (ACJIS). Information received from this system is made available by criminal justice agencies through the National Law Enforcement Telecommunications System (NLETS). Participating agencies in the NLETS include agencies from all 50 states, U.S. territories, federal agencies, select international agencies, and other partners serving law enforcement missions. The interface between ALERMS and ACJIS is managed through an interconnection security agreement (ISA) between BLM and Arizona Department of Public Safety (DPS). The interface between the systems relies on a local interconnection between BLM and AZ DPS firewalls located at a secure BLM-controlled facility.

The ALERMS receives event information from the DOI Incident Management Analysis and Reporting System (IMARS). Information received from the IMARS provides past event history including event location, involved persons and vehicles, associated property, event dispositions, and other event information. The interface between ALERMS and IMARS relies on the BLM General Support System (GSS) network for information sharing.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

Data collected in the system is used to record and document information related to public safety events, incidents and/or investigations on land/areas governed by the DOI, as well as tribal lands, and land/areas governed by the USDA, U.S. Forest Service (USFS). Data is held in a database repository controlled and maintained by authorized personnel. The PII collected is intended to be used to identify suspects, witnesses, victims, officers, investigators, and other involved parties, and will be used to verify the identity of individuals through validation with other external records systems and databases. PII is also used to obtain individuals' criminal activity and/or involvement in previous events, incidents and/or investigations from internal and external law enforcement systems for the purposes of identifying past criminal behavior.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office:

PII is shared within the BLM for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on BLM managed lands and/or against BLM personnel.

☒ Other Bureaus/Offices:

PII is shared with DOI bureaus and offices for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI and Tribal properties and/or against DOI and/or Tribal Members or employees.

☒ Other Federal Agencies:

PII is shared with other Law Enforcement agencies for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties. Information may also be shared between Law Enforcement and other Federal agencies. Information from this system is primarily shared with the USDA, USFS, the U.S. Department of Homeland Security and its subordinate agencies, and the U.S. Department of Justice and its subordinate agencies. The purpose of sharing data with other Federal agencies is to increase efficiency and probability of success of enforcement and/or investigative actions by cooperating agencies. For example, during an arson, drug smuggling, or other investigation information may be requested from this system that meets the parameters of their investigation, such as whether bureaus had any law enforcement contact with specific individual(s). If information is available and relevant, it would be shared with the requesting agency to assist in their investigation. If no relevant information were available, nothing would be shared. Information may be shared with external agencies as authorized and outlined in the routine uses section of the DOI-10, Incident Management, Analysis and Reporting System, SORN, which was published in the *Federal Register* at 79 FR 31974 (June 3, 2014), modification published 86 FR 50156 (September 7, 2021) and may be viewed at https://www.doi.gov/privacy/doi-notices.

☒ Tribal, State or Local Agencies:

PII is shared with other Law Enforcement agencies for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties, other properties and/or against DOI personnel and/or other personnel. Information may also be shared between Tribal, State and Local Law Enforcement Agencies. PII is shared only when necessary, which means only when the receiving agency has a lawful purpose and a bona fide need to know, as authorized and outlined in the routine uses section of the DOI-10, Incident Management, Analysis and Reporting System SORN, which was published in the *Federal Register* at 79 FR 31974 (June 3, 2014), modification published 86 FR 50156 (September 7, 2021) and may be viewed at https://www.doi.gov/privacy/doi-notices.

☒ Contractor:

PII is shared with DOI contractors involved in pre-employment screening and personnel security clearance work on behalf of the agency or bureau. These contractors are authorized to receive this information and have a Delegation of Authority from the Office of Personnel Management (OPM) to conduct this work on behalf of DOI. PII is shared with DOI contractors who facilitate technical operation of this "system" including maintenance, development, data validation, accuracy checking, archiving, and purging. These contractors conduct work on behalf of DOI and are authorized to have access to the information / data maintained in the system. Due to the sensitive nature of the data and the PII stored in this system, these contractors receive specific training courses designed to prevent unauthorized access to and or improper use of this data. These contractors are also required to sign FBI, CJIS, Security Addendums acknowledging the sensitivity of this information, the risks and responsibilities associated with accessing this data and the potential criminal and/or civil penalties associated with unauthorized access and/or improper use.

☒ Other Third-Party Sources:

Information that may contain PII may be shared through an agency public disclosure and release process after an incident and/or through the official Freedom of Information Act process. This would be based solely on the need to release information and would done in compliance with law, policy, and process. The purpose and benefit of releasing this type of information will always be weighed against the rights of individuals as compared to public benefit. PII is also shared with attorneys or court staff for judicial reasons. Information may also be shared with other third parties as authorized and described in the routine uses published in the DOI-10, Incident Management, Analysis and Reporting System, SORN which may be viewed at https://www.doi.gov/privacy/doi-notices. Exemptions have been claimed for this SORN.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes:

The BLM Office of Security Operations (OSO) utilizes the Mission Support Communication Center (MSCC) to perform criminal justice information queries as part of their pre-employment screening process when adjudicating new BLM employees for their background clearances. Part of this process requires information such as driver's license information, driver history, wants/warrants check, and criminal history reports. This information is provided by MSCC upon an official request from the OSO. PII is shared with DOI contractors involved in pre-employment screening and personnel security clearance work on behalf of the agency or bureau. These contractors are authorized to receive this information and have a Delegation of Authority from the OPM to conduct this work on behalf of DOI. Providing this information is voluntary and individuals may decline to provide. If an individual does not provide each item of requested information, OSO staff will not be able to complete the pre-employment screening process and

a background investigation, which will adversely affect the individual's eligibility for a national security position, eligibility for access to classified information, or logical or physical access. Withholding, misrepresenting, or falsifying information may affect an individual's eligibility for access to classified information, eligibility for a sensitive position, or individual's ability to obtain or retain Federal or contract employment.

The primary use of this system and the information is related to "in-person" field contacts of suspects/criminal violators by law enforcement officers. In this situation individuals are detained for the purposes of identification and investigation related to an event and are not able to decline to provide their identifying information.

Individuals in video/audio recordings will not have the opportunity to consent to the collection or use of the recording of their images or activities. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for audio or images captured during law enforcement operations or activities.

Officers make contact with subjects when out in the field. Part of this process is to run subjects through criminal justice information systems to check wants/warrants. This process is also required to generate local files, so officers have information when making contact with those same subjects in the future.

☐ No:

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement:

A Privacy Act Statement will be provided verbally by dispatchers upon request by individuals.

☒ Privacy Notice:

Notice is provided through the publication of this PIA and the DOI-10, Incident Management, Analysis and Reporting System, 79 FR 31974 (June 3, 2014), modification published 86 FR 50156 (September 7, 2021), which can be found at the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

☒ Other:

In some cases, such as for use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some DOI controlled areas may have signs posted informing individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for audio or images captured during law enforcement activities.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved through manual and automated queries of the system. Specific retrieval identifiers, including event number, location, date, officer number, name, date of birth, Social Security number (SSN), are used and the system uses keyword searches to search by any and all of the identifiers listed in Section 2, a of this PIA.

I. Will reports be produced on individuals?

☒ Yes:

Authorized users can manually run reports for investigative purposes. The following reports are available to authorized users: Event History Reports, Be On The Lookout (BOLO), Request for Identification Report, Criminal History Report, and Missing Person (also called Amber/Silver) report. A user is authorized based on the group role or roles assigned to the individual user. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. In addition, incident, supplemental, crash, arrest, ticket, and suspicious activity reports can be produced. Administrative reports may also be generated in response to audits, oversight, and compliance. These reports may be shared with other Law Enforcement Agencies for criminal justice, and investigative purposes.

☐ No

Section 3. Attributes of System Data

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

The system provides basic accuracy checking. The individual collecting the data will verify the accuracy of data collected in accordance with policy and procedures as defined by each participating organization. Supervisors will also review data for accuracy through an established Quality Assurance Program.

DOI is committed to protecting the privacy, civil liberties, and other legal rights of the American people to the greatest extent possible consistent with the DOI mission and operational requirements. DOI fulfills this responsibility through policy, monitoring, training, and oversight of the Department's privacy and civil liberties operations and participation in the information sharing environment (ISE). DOI provides redress in a manner that is compatible with legal authorities and mission requirements to individuals whose privacy, civil rights or civil liberties may have been affected in the ISE, which includes complaints related to privacy, civil rights and civil liberties protected by the U.S. Constitution or other laws, and complaints alleging racial, ethnic, or religious profiling, or retention of information that has been expunged or determined to have been illegally collected. Redress inquiries are investigated, and erroneous information or

deficiencies are corrected to ensure data integrity and protections for individual privacy, civil rights, and civil liberties. DOI procedures for complaints or requests to amend records that implicate protected information are outlined in the DOI Privacy Act regulations at 43 CFR 2.246, in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and the DOI ISE Privacy Policy. Individuals may also submit a complaint or a request to correct erroneous information in writing to the DOI ISE Privacy Official, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, D.C. 20240. To see the DOI Privacy Policy for the ISE or for additional information, visit the DOI Privacy and Civil Liberties website at https://www.doi.gov/privacy/privacy-civil-liberties.

B. How will data be checked for completeness?

The system provides basic completeness checking on individual fields for formatting and content. The individual collecting the data will verify the completeness of data collected per policy and procedures defined by each participating organization. Supervisors will also review data for completeness through an established Quality Assurance Program. The Quality Assurance Program will ensure that all personal data entered is complete and accurate to include name, date of birth, SSN, other individual identifiers, vehicle plates, vehicle identification numbers, and personal property information.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Individual users, including supervisors, are responsible for ensuring the data is current. Provided information is submitted to criminal justice information systems for validation and currency.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records retention schedules have been reviewed and discussed with the BLM Records Board and Bureau Records Officer. At this time, the records contained within this system do not match any existing records retention schedules. Records retention schedules will be developed or updated to include the records within this system. The records within this system will be treated as permanent until the records are scheduled and an appropriate disposition authority has been assigned and approved by NARA.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The records contained within this system will be treated as permanent until the records are scheduled and an appropriate disposition authority has been assigned and approved by NARA. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and Departmental policies. Archival and disposition of records will be accomplished within the automated records retention functions built in the system and procedures will follow guidance by NARA, applicable legislation such as the Federal Records Act, and Departmental guidance.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is risk to the privacy of individuals due to the amount of sensitive PII maintained for law enforcement events and incident reports, law enforcement investigations, and law enforcement personnel and training records. The risks are mitigated by controls implemented to limit unauthorized exposure of PII. Only authorized personnel with proper credentials can access the records in the system. DOI requires two-factor authentication for network and system access; system access is based on least privilege access and role-based access controls; access control lists were created and segmented; users cannot view information for other users unless specifically authorized. The system has been designed and built based on compliance with NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. A Security and Privacy Assessment & Authorization has been conducted on the system to verify, validate, and monitor compliance of this system.

Privacy risks exist with authorized data sharing with other law enforcement organizations. Risks may include but are not limited to data integrity, loss of data and data confidentiality for data shared and controlled by other organizations. A Memorandum of Understanding (MOU) will be established with agencies and organizations to ensure adequate controls are in place to protect privacy. Some examples of these additional controls include the following:

- MOUs established between agencies defining system access rules and policies
- Utilizing encryption on data transmission and data at rest
- Utilizing Secure File Transfer Protocols for transmission of information
- Access restrictions to authorized officials
- Authorized use of information shared
- Limits on uses and additional sharing
- Retention periods and authorized destruction or return of information shared

There is also a privacy risk for the use of audio recording devices used for routine law enforcement purposes to enhance officer safety, promote cost savings, assist in crime prevention, and support law enforcement investigations. These recordings are used to record crime reporting by individual law enforcement officials and the public on properties and locations within the jurisdiction of the DOI and cooperating agencies, including Federal facilities, national monuments, National Parks, tribal lands, and public lands to include buildings, housing units, roadways, trails, and bridges/tunnels, and law enforcement offices and jail units; National Wildlife Refuges; national dams and hydroelectric power plants.

These devices may capture audio events occurring in real time as part of ongoing law enforcement operations, such as identifying persons involved in potential criminal activity, or persons or vehicles fleeing from law enforcement officials. Some devices may capture metadata about the audio such as time, location, and date the audio. Recordings could be used in any appropriate law enforcement investigation related to a potential criminal activity, including identification of suspects, and providing evidence that may be used in proceedings.

Some privacy concerns are that devices may collect more information that is necessary to accomplish law enforcement purposes. The devices are used only to support law enforcement activities and investigations, prevent crime, and enhance officer safety. Only the audio recordings needed to respond to unlawful activities or support investigations and prosecutions will be retained for use, all other audio not required for retention will be automatically overwritten or disposed of per policy.

Another concern is that the use of the audio recording devices may restrict First Amendment protected activities like freedom of speech or association. The recordings are used to detect, deter, and investigate criminal activity and enhance officer and citizen safety. First Amendment activities will not be recorded for the sole purpose of identifying and recording the presence of individual participants engaged in lawful conduct. First Amendment activities may be recorded, however, for purposes of (1) documenting violations of law or civil wrongs; (2) aiding future coordination and deployment of law enforcement units; or (3) training; or (4) to mitigate or relieve overcrowding to enhance public safety.

Maintaining records without an approved records disposition could present a risk of unauthorized disposal of records. This risk is mitigated by consulting with a BLM Records Administrator or Records Manager to assist in determining a new schedule and obtaining the necessary approval from the National Archives Records Administration (NARA). In the interim, ensuring all unscheduled records are treated as Permanent and must not be destroyed, or otherwise dispositioned, until a confirmed NARA-approved Records Schedule is implemented with a disposition authority. Controls have also been implemented on limiting the retention of records maintained in this system to only that which is the minimum necessary for law enforcement purposes and establishing specific use policy and rules of behavior for the use of these unscheduled records.

There is a risk that information may be used outside the scope of the purpose for which it was collected. Personnel with access to recorded material and digital evidence will be subject to strict DOI policy, bureau policy, and Privacy Act standards. BLM employees and contractors must take privacy, security, and records management training prior to being granted access to BLM information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Failure to protect PII captured in digital evidence, to include the mishandling or misuse of this PII may result in criminal, civil and administrative penalties.

The ALERMS is undergoing a formal Assessment and Authorization and is anticipating an Authority to Operate in accordance with FISMA and NIST standards. This system is rated as FISMA moderate based upon the type of data, and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity

sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training. All employees must agree to DOI Rules of Behavior before being allowed to access the DOI network or any information systems. A general warning banner is displayed upon first logging into the DOI network that informs users that misuse of any system may subject employees to penalties.

There is a risk that individuals may not know how to seek redress or correction of their records. Individuals seeking redress may submit requests for correction through established procedures outlined in DOI Privacy Act regulations at 43 CFR 2.246 and in the Contesting Records Procedures section of the DOI-10 SORN. The DOI Privacy and Civil Liberties web page at https://www.doi.gov/privacy/privacy-civil-liberties also provides information on how individuals may submit a complaint or a request to correct erroneous information. However, DOI has exempted certain law enforcement records from one or more provisions of the Privacy Act under 5 U.S.C. 552a(j)(2) and (k)(2), in order to preclude an individual subject's access to and amendment of information or records related to or in support of an investigation.

There is a risk that the system may collect, store, or share more information than necessary, or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Records schedules will be developed for the records contained within the system. Following the records being scheduled and an appropriate disposition authority being assigned and approved by NARA, records will be disposed according to the applicable retention schedules. Until such time, records will be treated as permanent.

There is risk that data from different sources may be aggregated and may provide more information about an individual. This data may become outdated or inaccurate. This system supports law enforcement activities. Due to the nature of law enforcement operations and investigations, data collected about individuals from sources may be aggregated during the course of an investigation. Some mitigation occurs at the time of entry through data validation. Records are disposed based upon the records management schedule. Law enforcement records are created based upon the available information at the time, which may not be complete and precise. Through the course of an investigation additional records are created. The judicial process requires the law enforcement bureau/agency to provide records at the direction of a court and redress or correction of the records can be available through these proceedings (for example discovery, depositions, trial). Records are subject to release through the Freedom of Information Act. Supplemental reports can be added to the record.

There is a risk that individuals may not have notice regarding the collection of information, the purposes for collection or how the information will be used. Notice is provided through the

publication of this privacy impact assessment, the IMARS privacy impact assessment, and the published DOI-10 IMARS SORN.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes:

The system was developed with the purpose of collecting and storing PII to support and enhance the safety of law enforcement and administrative resource staff performing the mission of the BLM, DOI and cooperating agencies. The use of the system and the data is both relevant to the mission and necessary for the accomplishment of the mission.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☒ Yes:

This system is associated with records in DOI's law enforcement records management system, and/or criminal justice information systems. Data in these systems may be obtained from multiple sources instead of the individual. There is risk that data from different sources may be aggregated and may provide more information about an individual. This data may become outdated or inaccurate. Mitigation occurs at the time of entry through data validation. Records will be disposed based upon the records management schedule, once approved.

☐ No

C. Will the new data be placed in the individual's record?

☒ Yes: *Explanation*

Recorded data collected in support of law enforcement efforts may include PII collected from individuals that are contained in incident reports and used for official purposes. Those case files are in DOI's law enforcement records management system and are associated with individuals.

☐ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☒ Yes: Information contained within the system could be used to assist law enforcement with identifying individuals during investigations and prosecutions.

☐ No

E. How will the new data be verified for relevance and accuracy?

Users of the system are responsible for the relevance and accuracy of the data. Supervisors will also review data for accuracy and completeness during quality control reviews and investigations, which may include the subject.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.

Criminal justice information and open-source data on individuals related to incidents and/or events is obtained and consolidated from government and law enforcement organizations and systems. Methods used to limit exposure of PII:

- Role-based access controls for authorized personnel with proper DOI credentials
- Least privilege access
- Users cannot view information for other users unless specifically authorized
- Access Control Lists
- MOUs established between Agencies defining system access rules and policies
- Limiting information at the source (connection) deployed to outside agencies
- Utilizing encryption on data transmission and data at rest
- Utilizing Secure File Transfer Protocols for transmission of information
- System access is restricted through network firewalls on the BLM GSS

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users – users will have direct read/write access to data within the system.
☒ Contractors – access to data within the system will be incidental and controlled. Contractors will not have direct/un-monitored access to data.
☒ Developers – access to data within the system will be incidental and controlled. Developers will not have direct/un-monitored access to data.
☒ System Administrator – system administrators will have direct read/write access to data within the system.
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access requests for users are initiated by authorized bureau/office personnel on a need-to-know basis for information that is needed to perform an official function. A representative will evaluate the request and follow procedures to determine and grant individuals access to the system and data. Least privileges determine that only the minimum levels of access to perform

job functions are granted to users based on the users' job requirements. Role based security further limits access to system resources and data based on the users' role in the system.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes.

Contractors are responsible for designing, developing and maintaining the system. Privacy Act contract clauses are included in all contractor agreements in accordance with applicable DOI policies and regulations, and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a).

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The purpose of the ALERMS system is to track law enforcement and administrative field events including involved persons and vehicles. The data contained in the system will be used for administrative purposes and law enforcement purposes including field activities, investigations, and prosecutions. The nature of the system will include identifying individuals and associated criminal justice information about those individuals. The content stored within the system can provide location information individuals at the time of field events. The data collected may include physical attributes of an individual (including text, photos, and video), personal and professional physical addresses, telephone numbers, any associated information, and other PII listed in Section 2.A.

The ALERMS provides the capability to identify, locate, monitor, and audit the individuals based on a variety of criteria, including individual names; usernames; passwords; email addresses; phone numbers; sign on information; and internet protocol (IP) addresses. The ALERMS system has auditing and security features to enable reports to track and monitor user actions within the system. Since the nature of the system is storing event data associated with law enforcement and administrative personnel, the ALERMS creates reports and audit logs including username, time and date of logon, records accessed, records created, records deleted, information shared, and many other user and elevated actions.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The ALERMS automatically audits and logs username, date/time of log-in, as well as account changes and database including creation, modification, enabling, disabling, and removal for:

1) ALERMS access and user accounts to a database table, which triggers an automatic addition to an audit trail which administrators can access at any time for review and verification, and

2) ALERMS possesses the ability to integrate through an application programming interface automated auditing tools such as Splunk, which triggers an automatic email notification to system administrators for review and verification and the potential for automated auditing and reporting.

M. What controls will be used to prevent unauthorized monitoring?

Access granted to individuals using unique usernames and password combinations; each person granted access to the system must be trained and individually authorized to use the system. ALERMS also logs events including user login/logout, searches, views, and data alterations, which are reviewed on a regular scheduled basis. All users must accept the DOI Rules of Behavior before accessing the system and follow established internal security protocols. ALERMS users are required to complete Annual Training including the following Cybersecurity/Federal Information Systems Security Awareness; Privacy; Records Management and Controlled Unclassified Information training. In addition to the minimum requirements for all users, any users with elevated accounts for system administration must also complete Annual Role Based Security (RBST) training and Annual Role Based Privacy (RBPT) training.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- [x] Password
- [x] Firewall
- [x] Encryption
- [x] User Identification
- [ ] Biometrics
- [x] Intrusion Detection System (IDS)
- [x] Virtual Private Network (VPN)
- [ ] Public Key Infrastructure (PKI) Certificates
- [x] Personal Identity Verification (PIV) Card
- [ ] Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- [x] Periodic Security Audits
- [x] Backups Secured Off-site
- [x] Rules of Behavior
- [x] Role-Based Training
- [x] Regular Monitoring of Users' Security Practices
- [x] Methods to Ensure Only Authorized Personnel Have Access to PII
- [x] Encryption of Backups Containing Sensitive Data
- [x] Mandatory Security, Privacy and Records Management Training
- [ ] Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The State Director, BLM Arizona, is the Information System Owner and the official responsible for oversight and management of security and privacy controls and the protection of agency information processed and stored in the system. The Information System Owner and Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect the privacy, civil rights, and civil liberties in compliance with Federal laws and policies for the data managed, used, and stored in the system. These officials and authorized personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as addressing complaints and providing redress, in consultation with BLM and DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ALERMS Information System Owner is responsible for oversight and management of the system security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures.

BLM is responsible for ensuring that all employees with access to a system of records are aware of the requirements of the Privacy Act (5 U.S.C. 552a) and the Departmental Privacy Act regulations at 43 CFR Part 2, Subpart K for the handling, disclosure, and alteration of such records and the possibility of criminal penalties for improper disclosure. All DOI employees and contractors are responsible for safeguarding privacy, reporting any compromise of PII and complying with Federal and Departmental privacy requirements.