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: Digital Evidence Management System (DEMS)
Bureau/Office: Department of the Interior
Department wide PIA for digital evidence management support law enforcement use of body worn camera, closed circuit television, and other digital evidence.
Date: March 12, 2021
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, Reston VA 20192

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 Digital Evidence Management System (DEMS) is an enterprise, commercial-off-the-shelf,end-to-end law enforcement camera and digital evidence management system. Body worn cameras, dash-mounted vehicle cameras, handheld cameras, and closed circuit television are camera systems currently used by law enforcement officers in the performance of their duties. Still images and other digital evidence are also obtained and collected from the public as evidence during an investigation. Digital evidence can come from a number of sources and is not limited to body worn cameras. The DEMS will provide an integrated system of cameras, compatible software and mobile applications to enable law enforcement officers to download, catalogue, tag, manage, and store the digital evidence in a FedRAMP approved, cloud-storage system.

The system includes:

- Collecting and uploading content in any file format, from any device;
- Transferring the data by automatically uploading content from body worn camera devices and hard drives;
- Managing - Keep information organized and tag it with the correct metadata;
- Retrieving - Find evidence quickly with search features;
- Sharing - Grant access to authorized persons, like prosecutors, or share content with a secure link;
- Scalable - Increase storage space as needed;
- Effortlessly tag video with correct metadata;
- Integrating with bureau computer-aided dispatch and the DOI Incident Management, Analysis and Reporting System (IMARS) records management system through automation of the process of tagging videos with complete, correct metadata;
- Ensure evidence receives the appropriate automatic retention period; and
- Redact data in response to Freedom of Information Act requests for information.

DEMS may use mobile applications designed to upload video, photo, and audio recordings captured on the users' mobile devices (smartphone and tablets) directly into a secure cloud-based metadata storage system. They also allow an agency to register, assign, and reassign DEMS devices and allow a user to wirelessly interact with a camera to view recorded videos, preview live video capture, and apply metadata to video files. Bureaus using the DEMS may ormay not make use of the mobile applications as part of the law enforcement activities. DEMS Mobile application should only be installed and utilized on DOI government issued mobile devices used for law enforcement purposes. These devices meet DOI requirements for IT security protection.

C. What is the legal authority?

DOI authorities: Uniform Federal Crime Reporting Act, 28 U.S.C. 534; Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458); Homeland Security Act of 2002

(Pub. L. 107–296); USA PATRIOT ACT of 2001 (Pub. L. 107–56); USA PATRIOT Improvement Act of 2005 (Pub. L. 109–177); Homeland Security Presidential Directive 7—Critical Infrastructure Identification, Prioritization, and Protection; Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employeesand Contractors; Criminal Intelligence Systems Operating Policies, 28 CFR part 23.

National Park Service U.S. Park Rangers, U.S. Park Police: 54 U.S.C. 100101, 54 U.S. Code § 102701; Federal Register 44876 (October 13, 1976)); Act of August 5, 1882 (22 Stat. 243); Act of March 17, 1948 (62 Stat. 81) (Also codified as D.C. Code § 5-201 et seq).

Bureau of Land Management: 43 USC 1733 – Enforcement Authority – Federal Land Policy & Management Act of 1976 (a); The Wild Free-Roaming Horse and Burro Act (16 U.S.C 1331-1340) may be enforced only by special agents and must be done in cooperation with theBureau of Land Management.

Fish and Wildlife Service: Lacey Act and Lacey Act Amendments of 1981 (18 U.S.C. 42, 16 U.S.C. 3371-3378); Migratory Bird Treaty Act (16 U.S.C. 703-711); Upper Mississippi River Wildlife and Fish Refuge Act (16 U.S.C. 721-731); Bear River Migratory Bird Refuge Act (16 U.S.C. 690-690i); Migratory Bird Hunting and Conservation Stamp Act (16 U.S.C. 718-718h and 718j); Bald and Golden Eagle Protection Act (16 U.S.C. 668-668d); Fish and Wildlife Actof 1956 (16 U.S.C. 742a-742d and 742e-j-2) (includes airborne hunting prohibitions); Fish and Wildlife Improvement Act of 1978 (16 U.S.C. 712); Fish and Wildlife Recreation Act (16 U.S.C. 460k-460k-3); National Wildlife Refuge System Administration Act (16 U.S.C. 668dd-668ee); Endangered Species Act (16 U.S.C. 1531-1544); Marine Mammal Protection Act (16 U.S.C. 1361-1384, 1401-1407); Antarctic Conservation Act of 1978 (16 U.S.C. 2401; 2412); Archaeological Resources Protection Act (16 U.S.C. 470aa-11); African Elephant Conservation Act (16 U.S.C. 201-4244); Wild Bird Conservation Act (16 U.S.C. 4901-4916); Rhinoceros and Tiger Conservation Act (16 U.S.C. 5301-5306).

Bureau of Indian Affairs: 25 U.S. Code § 2803 - Law enforcement authority; Tribal Law and Order Act of 2010 (Pub. L. 111-211).

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:

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
(UII): 010-000002392 00-24-01-02-02-00
Digital Evidence Management System (BWC-DEMS) Security Plan

☐ 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.*
Axon View	Axon View is a mobile application for mobiledevices (smartphones and tablets) that allows an agency user to wirelessly interact with a camera to view recorded videos, preview live video capture, and apply metadata to video files. It wirelessly connects with a camera to provide instant playback of unfolding events in the field. The user of the application sees what the camera sees. The Axon View application falls within the DEMS security boundary. A separate PrivacyThreshold Analysis (PTA) has been conducted for this application. The Axon View mobile application should only be uploaded and utilized on governmentissued mobile devices. These devices meet DOI requirements for IT security protection.	Yes	Axon View does not retain PII or video files on the mobile device, but only views video stored on a paired camera. It cannot transfer, delete or alter original video files that are stored on a camera. Physical access to the camera is required to initiate pairing with Axon View and requires persistent close proximity to a camera to provide functionality.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Axon Capture	Axon Capture is a mobile application for mobile devices (smartphones) that allows an agency user to upload video, photo, and audiorecordings captured on the users' smartphone directly to Evidence.com, the secure cloud- based metadata storage system. Rather than utilizing a separate recording device, such as a body-worn camera or in-vehicle camera, Axon Capture uses the recording capabilitiesof the smartphone. The user must be signed into an agency prior to uploading the digital data to their Evidence.com tenant. The evidence will be stored in the Axon Capture application beforebeing uploaded to Evidence.com. Once the user has the feature enabled in their Axon Capture settings, the user can import video, photo, and audio data from their smartphone digital library or the default repository on their device to Axon Capture, where it can then be uploaded into the user's Evidence.com tenant. The Capture application allows the user to add tags, titles, or GPS coordinates to any recording prior to uploading the data directly into Evidence.com. The Axon View application falls within the DEMS security boundary. A separate PrivacyThreshold Analysis (PTA) has been conducted for this application. The Axon Capture mobile application shouldonly be uploaded and utilized on government issued smartphones. These devices meet DOI requirements for IT security protection.	Yes	The Axon Capture application allows the user to capture, store, process, and upload video/audio data, which may contain PII, from the user's government issuedmobile device. Rather than use a separate camera device, such as a body worn camera or in-vehicle camera, to capture digital data, the user's government issued mobiledevice is the camera.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Axon Device Manager	Axon Device Manager (ADM) is a mobile application for mobile devices (smartphones and tablets) that allows an agency user to register, assign, and reassign Axon devices. In order to use the ADM application, the role of the user in Evidence.com must have a Device Administration permission, or Conducted Electrical Weapons (CEW) Administration permission, or both permissions set to 'Allowed' to use the ADM application. Though ADM is the preferred method for registering, assigning, and reassigning Axon devices, devices can also be registered, assigned, and reassigned directly in Evidence.com. The Axon View application falls within the DEMS security boundary. A separate Privacy Threshold Analysis (PTA) has been conducted for this application. The Axon Device Manager mobile application should only be uploaded and utilized on government issued mobile devices. These devices meet DOI requirements for IT security protection.	No	ADM does not create, collect, use, process, maintain or disseminate PII or specific information about individuals. The ADM application is used to register, assign, or reassign Axon devices which do collect, use, process, maintain, and disseminate PII, but doesnot itself collect, process, store, or interface with any of this collected data.

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

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI-10, Incident Management, Analysis and Reporting System (IMARS), 79 FR 31974, June 3, 2014.

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name	☐ Religious Preference	☒ Social Security Number (SSN)
☒ Citizenship	☐ Security Clearance	☒ Personal Cell Telephone Number
☒ Gender	☒ Spouse Information	☒ Tribal or Other ID Number
☒ Birth Date	☐ Financial Information	☒ Personal Email Address
☒ Group Affiliation	☒ Medical Information	☐ Mother's Maiden Name
☒ Marital Status	☐ Disability Information	☒ Home Telephone Number
☒ Biometrics	☐ Credit Card Number	☒ Child or Dependent Information
☒ Other Names Used	☒ Law Enforcement	☒ Employment Information
☒ Truncated SSN	☒ Education Information	☒ Military Status/Service
☒ Legal Status	☒ Emergency Contact	☒ Mailing/Home Address
☒ Place of Birth	☒ Driver's License	☒ Race/Ethnicity

☒ Other: Digital evidence includes audio, video, still images, or other media that has been captured in the normal course of law enforcement duties. PII is captured on law enforcement camera systems when the recording device is activated during law enforcement citizen interactions. Data recorded is directly related to law enforcement activities and emergency response, and may include video images of people, driver licenses, personal information verbally requested for the purposes of violation notices and/or arrests during a lawful contact, and criminal history information provided over the radio by the dispatch communications center. Information may also be obtained from publicly available sites, witnesses, concerned citizens, and the general public's personally owned devices. Digital evidence may be associated with PII collected by lawenforcement officials while taking statements or during the course of an investigation and may include the following information: Social Security numbers (SSNs), driver's license numbers, vehicle identification numbers, license plate numbers, names, home addresses, work addresses, telephone 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. Victim, juvenile, witness, criminal, and informant information may be captured. The system contains images and videos collected from audio/visual recording devices such as surveillance cameras, closed circuit television located at DOI facilities for security and/or law enforcement operations, a mobile video

recorder installed on a patrol vehicle and a wearable video recorder (i.e., body-worn cameras) or a DEMS mobile application authorized for law enforcement operations.

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: PII is captured on law enforcement camera systems when the recording device is activated during law enforcement citizen interactions. Data recorded is directly related to law enforcement activities and emergency response, and may include video images of people, driver licenses, personal information verbally requested for the purposes of violation notices and/or arrests during a lawful contact, and criminal history information provided over the radio by the dispatch communications center. Information may also be obtained from publicly available websites, witnesses, concerned citizens, and the general public providing images and recordingsfrom their personally owned devices.

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
☒ Other: Digital audio/video format dependent on the device.
Data feeds will be established using application programming interface (API) to exchange data between computer aided dispatch systems and department recordsmanagement system (IMARS).

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

PII is used for official law enforcement purposes. The system provides law enforcement employees mobile video recording capability (body cameras, in-car cameras, CCTV) to document officer-citizen encounters while engaged in patrol functions. Digital evidence is used in law enforcement activities on lands/areas governed by the DOI as well as tribal lands. It is used to support the investigation and prosecution of criminal activity and violation of laws on DOI lands and/or against DOI personnel.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.* PII is shared within Bureaus for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
PII is shared within DOI Office of Law Enforcement and Security (OLES) and other DOI Bureaus for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
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 DOI Law Enforcement and other Federal agencies as authorized and described in the routine uses published in the DOI-10 IMARS system of recordsnotice, which may be viewed at:
https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*
PII is shared with Tribes for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties which might include Tribal lands. Information may be shared with Local agencies for law enforcement purposes. For example some National Parks use CCTV and may share data with local law enforcement depending on the nature of the event and who has jurisdiction.

☒ Contractor: *Describe the contractor and how the data will be used.*
PII is shared with DOI contractors to facilitate system operation.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*
PII is 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-10IMARS system of records notice, which may be viewed at:
https://www.doi.gov/privacy/sorn.

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

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Due to the purpose and nature of the system, to support law enforcement operations and investigations, individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. 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 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.

Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements from a sexual assault victim, when a juvenile is involved, or as stipulated by policy.

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

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*
Notice is provided through this PIA and the publication of the DOI-10, Incident Management, Analysis and Reporting System (IMARS), 79 FR 31974, June 3, 2014.

☒ Other: *Describe each applicable format.*

Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but given the unpredictability of law enforcement interactions orencounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of NPS personnel or third parties. Therefore, DOI also provides general notice to the public through this PIA.

NPS policy (RM-9) requires National Parks that utilize CCTV post a public notice on the Superintendent's Compendium for that Park that includes a CCTV Policy Statement informing the public on the use of CCTV for official law enforcement and security purposes.

Body worn cameras have indicator lights on when they are recording. In addition, uniformed officers, who the general public would recognize as having law enforcement authority, wear cameras visible to the public on their shirt or jacket.

☒ None

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 that inform individuals of surveillance activities, but given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of NPS personnel or third parties.

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

Digital evidence is tagged (labeled) for ease of search and retrieval. Generally, they are tagged as evidence or non-evidence for records retention purposes. Additional tagging associated with an incident, individual's name, date of incident, or other attribute may also occur.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Detailed information can be viewed by authorized users. Administrative reports may also be generated in response to audits, oversight, and compliance. Digital evidence can be linked to an incident which routinely has an associated individual. Metadata that is associated with the incident report for an investigation that is maintained in the recordsmanagement system (IMARS) may be available through the Freedom of Information Act subject to exemptions under the Privacy Act for law enforcement records.

☐ No

Section 3. Attributes of System Data

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

The majority of images captured through the various digital evidence media are from DOI law enforcement cameras in real time. Recorded data collected that relates to individuals for an authorized purpose is verified by the law enforcement dispatch communication center through a General Agreement. Use of an application programming interface (API) is used for data validation and transfer. Software would prevent the altering, tampering, or destruction of the original recording.

For external sources, law enforcement officials will verify the accuracy of data collected per policy and procedures defined by each participating organization. Supervisors will also reviewdata for accuracy during the investigation process.

B. How will data be checked for completeness?

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 during the investigation process, which may include subject or witness interviewsand verifying information with other law enforcement agencies and organizations.

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

Video recordings used for law enforcement purposes are taken in real time. Recordings have adate and time stamp when they are created.

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

Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, which provides that recordings of a non-evidentiary value will be destroyed after 30 days. Videos associated with criminal incidents in the database will be maintained as evidence according to the specific incident's disposition schedule. Video disposed of in accordance with the following schedules.

Where the recordings are for routine security measures and surveillance, and are necessary for day-to-day operations but not suitable for long-term preservation, use Departmental Schedule **DAA-0048-2015-0002-0001**. These recordings are of a non-evidentiary value and will be automatically destroyed after **30 days**. NOTE: In the event of a security breach or other such incident, or in the event that a recording is identified as otherwise relevant to a particular legal or investigative case file, the recording will be included as part of the case file. The applicable recordings will be copied from the system, retained and used as part of an NPS investigative case file and will be retained according to the NPS records disposition schedules **N1-79-08-002** as follo s

Item 2A2 where the recording is added to Significant investigation files - PERMANENT. Transfer to NARA 15 years after closure of investigation file. Criteria for selecting "significant"cases are as follows:

- incidents (natural or man-made) that cause significant or permanent damage to, or loss of, a cultural or natural resource with great monetary, cultural, scientific, or historical value,
- creation of new protection or safety procedures that constitute a new way of providing services,
- new policies that change the nature of the activity,
- "first of kind" events that establish precedents,
- subject of widespread media attention or Congressional scrutiny, or

- substantiated Native American Graves Protection and Repatriation Act (NAGPRA), Archeological Resources Protection Act (ARPA), and Indian Arts and Crafts Board (IACB) claims.

Item 2B where the recording is added to Major Investigation cases. Includes major accident/ incident investigations or activities. This category applies to offenses that are generally criminal in nature. It also applies to unsubstantiated NAGPRA, ARPA, and IACB claims. Destroy/Delete25 years after closure. Item 2C where the recording becomes part of Minor Investigation files. Such as minor incidents, investigations, or activities, offenses that are generally not criminalin nature, and cases that do not apply to natural or cultural resources. Destroy/Delete 7 years after case closure.

Data of evidentiary value will be transferred into IMARS. IMARS records are retained and disposed of in accordance with Office of the Secretary Records Schedule, Item 8151, Incident, Management, Analysis and Reporting, which was approved by the National Archives and Records Administration (NARA) (N1-048-09-05), and other NARA approved bureau or office records schedules. Incident data will be cut-off when an incident is closed off. The data will be archived 20 years after cut-off and destroyed 50 years after archiving. Non-incident data includes data relating to the user/officer and their unit of assignment, badge number, training, qualifications, etc. This data will be cut-off after the user/officer retires, resigns, leaves the DOI, or is assigned to a position that no longer requires access to IMARS. This data is archived three years after cut-off and destroyed 50 years after archiving.

Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, which provides that recordings of a non-evidentiary value will be destroyed after 30 days. Videos associated with criminal incidents in the database will be maintained as evidence according to the incident's disposition schedule.

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

Approved disposition methods include shredding or pulping for paper records, and degaussingor erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1. Archival and disposition of records will be accomplished within the automated records retention functions built in the system, and procedures will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, and Departmental guidance.The procedures are documented in the DEMS Records Management Plan and approved by NARA. Transitory, non-evidentiary records will be disposed after 30 days of retention.

Evidence destruction is completed by the evidence custodian following the adjudication of the case, receipt of a court order, or as part of evidence inventory management. Deletion/destructionof digital files is documented in the digital evidence management

system for non-evidentiary records. Procedures for disposal/destruction of evidentiary records is specified in Department and Bureau policy.

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 a risk to the privacy of individuals in DEMS due to the amount of sensitive PII that may be captured and used or maintained for law enforcement incident reports, law enforcement investigations, and citizen encounters. The risks are mitigated by controls implemented to limit unauthorized exposure of PII. DEMS is rated as a FISMA moderate system based upon the type and sensitivity of data and requires security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. The privacy controls are utilized to protect individual privacy, including limiting access to images or video feed that identify individuals or to specific events or investigations that are linked to individuals, to authorized users and law enforcement officials. 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.

Privacy risks exist with data sharing with other law enforcement organizations related to the unauthorized sharing, data integrity or loss of data. DEMS supports law enforcement activities at DOI and PII is shared with other Law Enforcement agencies as part of the information sharing environment, for the purpose of investigation, apprehension, recordkeeping, and arrest and/or conviction for crimes committed on DOI lands and/or against DOI personnel. The system provides law enforcement officials mobile video recording capability to document officer-citizen encounters while engaged in patrol functions, which are used in law enforcement activities on lands/areas governed by the DOI as well as tribal lands. DOI establishes information sharing agreements with partners for any sharing outside DOI. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the DOI-10 IMARS system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn. Examples of controls to mitigate these risks include:

- 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 a privacy risk for the use of audio/visual recording devices, such as body cameras, dashboard cameras, and hand-held cameras. These recording devices are used for routine law enforcement purposes to enhance officer safety, promote cost savings, assist in crime prevention, and support law enforcement investigations. These cameras may be worn by

DOI bureau and office law enforcement officials, placed on the dashboard of law enforcement vehicles, or used by individual law enforcement officials on properties and locations within the jurisdiction of the DOI. These locations include Federal facilities, national monuments, national parks, tribal lands, National Wildlife Refuges, national dams and hydroelectric power plants, law enforcement offices and jail units, and public lands to include buildings, housing units, roadways, trails, and bridges/tunnels.

These devices may capture audio and images of persons, places and 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 such as audio, images or recordings which provide the time, location and date of the event. Users may use settings to zoom in for persons or objects of specific interest or pan areas of interest. Images or recordings could be used in any appropriate law enforcement investigation related to a potential criminal activity, including identification ofsuspects and providing evidence that may be used in proceedings.

Some privacy concerns are that devices may collect more information than is necessary to accomplish law enforcement objectives. The devices are used by authorized law enforcement officials to support law enforcement activities and investigations, prevent crime, and enhance officer safety, and provide training to promote safety and best practices. Only the images or video feed needed to support official law enforcement operations, respond to unlawful activities or support investigations and prosecutions will be retained for use. All other video feed not required for retention will be automatically overwritten or disposed of per DOI records retention policy.

Another concern is that the use of the audio/visual recording devices may restrict First Amendment protected activities like freedom of speech or association. First Amendment demonstrations will not be filmed for the sole purpose of identifying and recording the presence of individual participants engaged in lawful conduct. First Amendment demonstrations may berecorded where rangers/officers encounter them in the course of routine law enforcement activities to document arrests, to document violations of law or unlawful conduct.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. 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. Those with access to the system receive privacy, security, and records management training, both prior to the granting of access and annually thereafter. DOI employees and contractors must take privacy, security and records management training prior to being granted access to DOI 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. Disclosure of sensitive information or PII to unauthorized recipients, failure to protect PII, mishandling of PII or misuse of PII may result in criminal, civil, and administrative penalties.

DEMS will be hosted by a cloud service provider. There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The data collected by law enforcement cameras and uploaded into the evidence management system will be considered sensitive and will contain PII. The provider will implement protections and controls to restrict access to unauthorized parties, as will be required to attain the necessary FedRAMP Authority to Operate (ATO). The provider will be required to submit to additional security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information inaccordance with Federal and DOI privacy and security standards.

There is a risk that information may be used outside the scope of the purpose for which it was collected. Law enforcement personnel with access to recorded material and digital evidence will be subject to strict DOI policy, bureau policy, and Privacy Act standards. These law enforcement personnel will be required to take privacy, security and records management training prior to being granted access to system, and annually thereafter. They 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.

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. Additionally, controls are established in accordance with approved records retention schedules to ensure retention of images and video feeds does not exceed approved periods necessary for law enforcement purposes. DOI restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (30 days) in accordance with approved records retention schedules for routine surveillance motion picture and video recordings. The DOI policy and records retention schedules dictate proper disposal of recordings at the end of the retention period and establishes specific policy and rules of behavior for the use of these audio/visual recording devices. Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, Only data with evidentiary relevance will be uploaded into IMARS and retained beyond 30 days. This evidentiary data will be maintained according to the incident's disposition schedule. Video and audio recordings of non-evidentiary value is transitory and willbe destroyed after 30 days in accordance with approved records retention schedules for routine surveillance motion picture and video recordings.

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 related to external sharing of data with other Federal, state, Tribal, local, international law enforcement organizations and sharing incorrect, inaccurate or outdated records misidentification. The system incorporates secure communication using Transport Layer Security (TLS) for all transmission of data to the internal repository as well as external agency repositories. Interconnection agreements are established through IMARS and enable bureaus to share authorized data with other Bureaus and other law enforcement organizations. The service agreements ensure the proper documentation of the technical requirements for connectivity and compliance with secure communications for Federal Information Systems in accordance with NIST SP 800-47 “Security Guide for Interconnecting Information Technology Systems.” In addition, a continuous monitoring program is in place through boundary protection mechanisms as well as the data repository hosting facility.

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, published IMARS SORN, posted signs for areas that use CCTV, and the CCTV Policy Statements posted on National Park websites. The body-worn cameras are worn openly on the officer’s uniform. Case law has established that an in-vehicle camera is in a public area where there is no reasonable expectation of privacy and does not violate the law. No law or DOI policy requires a notification to the public of officers recording video in public spaces while performing their law enforcement duties.

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 Procedures section of the IMARS notice. 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 to the privacy of individuals with the use of the mobile applications due to the nature of law enforcement interactions with the public and the amount of PII that the mobile applications can access for viewing, processing and storage from videos, photos, audio, and metadata such as GPS data. The mobile devices use a combination of technical and operational controls to mitigate the privacy risks such as government approved encryption for storage, least privileges for authorized users of the system, and persistent close proximity to a camera for functionality. In addition, mobile applications are only installed and used on authorized government issued mobile devices that meet DOI requirements for IT security protection.

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: *Explanation*

The use of DEMS is necessary for the collection, transfer, management, retrieval, sharing, redaction, release, and records management associated with evidentiary and non-evidentiary data in support of law enforcement activities.

☐ No

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

☒ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

This system is associated with law enforcement records in IMARS, the DOI law enforcement system, and/or computer aided dispatch systems (CAD). Data in IMARS and CAD 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 are disposed based upon the records management schedule.

☐ 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 video relating to individuals that is contained in incident reports and used for official purposes. Those case files are located in IMARS and are associated with individuals. Digital content is tagged and associated with incidents that are associated with individuals.

☐ No

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

☒ Yes: *Explanation*

Digital evidence (images) 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?

Law Enforcement Officers and their supervisors are responsible for the relevance and accuracy of the data. Supervisors will also review data for accuracy and completeness during the investigation process, which may include subject or witness interviews and verifying information with other law enforcement agencies and organizations.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ 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
☒ Contractors

☒ Developers
☒ System Administrator
☐ Other: *Describe*

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

Access to DEMS is restricted by a role-based and least privilege principles. Access to the evidence management system requires an active DOI email account. Law enforcement officials require supervisor authorization to establish user accounts to access the system. Users will not have access to all data, they will have access to the data required to perform their duties based on their roles. System administrators will assign levels of access. DEMS supports law enforcement activities at DOI and shares PII with other Law Enforcement agencies as part of the information sharing environment, for the purpose of investigation, apprehension, recordkeeping, and arrest and/or conviction for crimes committed on DOI lands and/or against DOI personnel. DOI establishes information sharing agreements with partners for any sharing outside of DOI. Information from DEMS may be associated with an event or incident in IMARS and shared with DOI bureaus and offices and other law enforcement agencies through Interconnection Security Agreements, Memorandums of Understanding, or other information sharing agreement as part of the information sharing environment. The authorized sharing of information in support of law enforcement activities is described in the routine uses published inthe DOI-10 IMARS system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn.

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 will be involved in the development and maintenance of the system and Privacy Act contract clauses will be included in the contract.

☐ 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 DEMS is to provide surveillance in support of law enforcement operations, investigations and prosecutions. The nature of the system will include monitoring individuals as it provides law enforcement officials mobile video recording capability to document officer-citizen encounters while engaged in patrol functions, which are used in law enforcement activities on lands/areas governed by the DOI as well as tribal lands. The content within the system can provide the capability to identify and locate individuals. The data collected may include physical attributes of an individual, personal and professional address, telephone, any associated information, and other personally identifiable information such as SSN and DOB. Additionally, the system itself has audit features that monitor user activity within the system.

☐ No

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

Digital information including audio and video is captured from CCTV and various media. Digital information that is evidentiary in nature is collected. The data collected may include physical attributes of an individual, personal and professional address, telephone, any associated information, and other personally identifiable information such as Social Security number and date of birth. Non-evidentiary digital media is transitory and destroyed. The system audit features monitor user activity within the system and collect:

- Successful login
- Successful logout
- Unsuccessful login
- Unsuccessful logout
- Date/time of access
- Privileged system changes
- Accounts created, deleted or modified
- All password resets
    - Groups created, deleted or modified
    - Membership changes
- Permission or rights assignments
- All super user (administrator or root) activities on the service
- All rights or permission assignments
- Successful or Failed software patch or upgrades
- New services installed or started
- Restarts or resets
- Audit log configuration changes

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

The system itself has audit features that monitor user activity. Access controls, least privileges, rules of behavior, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to security and privacy training. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply. (For on premise or hybrid)

☒ Security Guards
☐ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. Physical controls are based on DOI controls and a set menu of controls from the cloud service provider. Once the system is implemented, this PIA will be updated based on security controls implemented.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. Technical controls may vary based upon a cloud, on premise, or hybrid solution/storage. This PIA will be updated once a cloud service provider is selected and the system is assessed.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site

☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ 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 Chief Law Enforcement, Security and Emergency Services (LESES), is the DEMS Information System Owner and the official responsible for oversight and management of the DEMS security and privacy controls and the protection of agency information processed and stored in the DEMS system. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in DEMS. These officials and authorized DEMS personnel are responsible for protecting individual privacy for the information collected, maintained, used, shared and disposed of in thesystem, and for meeting the requirements of the Privacy Act. The IMARS System Manager is responsible for providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with DOIprivacy officials.

DOI bureaus and offices using the system are responsible for designating bureau specific rolesand responsibilities. Unit level senior law enforcement officers (Chief, Chief Ranger) are responsible for issuing appropriate guidance, establishing procedures, adhering to department and bureau policy, reporting violations and investigation of violations.

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 DEMS Information System Owner and Information System Security Officer are responsible for daily operational oversight and management of the system's security and privacy controls, and 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 DEMS Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosureof PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with Federal policy and established DOI procedures.

The unit senior law enforcement officer (Chief, Chief Ranger) is responsible for overseeing the video recording and storage system, ensuring compliance with Bureau and Department policies.Each bureau and office is responsible for ensuring that all employees with access to a system ofrecords are aware of the requirements of the Privacy Act (5 U.S.C. 552a) and the Departmental Privacy Act regulations (43 CFR Part 2, Subpart K) concerning 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.