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: Enterprise Dispatch Management System (EDMS)
Bureau/Office: National Park Service, Visitor and Resource Protection
Date: May 24, 2022
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

B. What is the purpose of the system?

The National Park Service (NPS) owns and operates a suite of systems used to support nationwide law enforcement and emergency services dispatch management whereby federal employees, contractors, and visitors may report suspicious activity, security

related matters, and alleged violations of law related to the protection of NPS properties. This suite of systems is collectively referred to as the NPS Enterprise Dispatch Management System (EDMS). The NPS Office of Law Enforcement, Security and Emergency Services (LESES) is responsible for the governance and management of EDMSs across the NPS. LESES is conducting a privacy impact assessment (PIA) to identify and address privacy implications for the use of NPS dispatch management systems. This PIA covers the NPS dispatch management systems authorized by LESES in accordance with NPS LESES policies and procedures. NPS park units or offices are required to comply with governance, policies, procedures, and security and privacy control implementation under the direction of the NPS LESES EDMS Program Management Office (PMO). Any uses that are inconsistent or outside the scope of this PIA may result in corrective or administrative actions from the LESES EDMS PMO, including, but not limited to, revocation of Authority to Operate (ATO) for the unit or office dispatch management system and/or imposition of a requirement for the park or office to conduct and pursue separate PIA and ATO for the specific legitimate purpose and address any distinct privacy and security risks related to the specific use, as well as meet any additional privacy and security compliance requirements for the use of the technology and collection and maintenance of data within their system(s).

The EDMS consists of Computer-Aided Dispatch (CAD) systems, purpose specific dispatch consoles, 911 recorder systems, and license plate readers used internally by park commissioned Law Enforcement Officers (LEOs) and Dispatch Center staff throughout the NPS in daily operations to increase efficiency in receiving and facilitating emergency real-time responses to public and employee safety incidents. The dispatch consoles interface to two-way radio and phone systems allowing communication between the dispatch center and the field and create a continuous, chronological log of reports of daily activities. All radio and phone communication is recorded on the 911 recorder subsystem. These recordings are saved and allow for play-back for event reconciliation, records retrieval, and quality assurance.

Incident records are recorded into the CAD subsystem and exported to Department of the Interior (DOI) Incident Management, Analysis and Reporting System (IMARS). The CAD technology consists of commercially available software hosted by NPS with fail over between sites. The CAD collects and stores information on individuals who may be associated with an incident for purposes of response and investigation of the incident. These individuals are typically persons believed to be involved in or related to a particular incident, such as suspects, victims, witnesses, participants, employees, and building occupants and visitors.

Automated license plate readers (LPRs) are high-speed, computer-controlled video-only camera systems that are typically mounted on street poles, streetlights, highway

overpasses, or vehicles at ingress/egress points or selected locations throughout NPS properties. LPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data includes photographs of the vehicle and may include images of the driver and/or passengers. Enhanced LPR functionality enables criminal investigators with only limited information to identify suspect vehicles in furtherance of a law enforcement investigation.

The EDMS CAD subsystems interface with the National Crime Information Center (NCIC) through the State Law Enforcement System (SLES) in the state(s) where the park unit(s) or office(s) are located. Each State law enforcement bureau or division administers their respective SLES. This will allow Law Enforcement Security Emergency Services (LESES) personnel and dispatch operators to perform one entry searches of multiple law enforcement and emergency service databases, providing substantially faster data gathering of relevant information. License plate readers interface to the SLES; however, license plate readers only return a status indicator identifying if there is LE or public safety activity of interest associated with the license plate and do not capture additional data from the SLES.

The interface with IMARS is uni-directional with data uploaded to IMARS from the CAD subsystems, but data from IMARS is not downloaded to the EDMS subsystems. The dispatch consoles and 911 recorder subsystems do not interface with IMARS, NCIC or SLES.

The organization of historical data and the ability to immediately maintain and recall information along with access to the above-mentioned information systems will directly result in added safety to LESES and non-LESES staff, as well as the general public and park visitors. By utilizing the EDMS system, Law Enforcement staff will be able to handle emergency and hazard incidents in a safe and efficient manner consistent with national and department standards.

This information will be used to collaborate with Federal, state and local law enforcement activities. EDMS will enhance the following abilities:

- Prevent, detect, and investigate known and suspected criminal activity.
- Protect natural and cultural resources.
- Capture, integrate and share law enforcement and related information and observations from other sources.
- Identify needs (training, resources, etc.).
- Measure performance of law enforcement programs and management of emergency incidents.
- Analyze and prioritize protection efforts.

- Justify requests and expenditures.
- Assist in managing visitor use and protection programs.
- Training (including, incorporating into Federal Law Enforcement Training Center programs)
- Investigate, detain and apprehend those committing crimes on DOI lands.
- Investigate and prevent visitor accident injuries on DOI lands

The system is managed by NPS employee and contractor staff and is accessible for use by commissioned LEOs and dispatch operators.

C. What is the legal authority?

- 28 C.F.R. § 20 - Criminal Justice Information Systems; DOI DM 446 Chapter 14
- 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:

- UII Code: 010-000000590
- System Security Plan (SSP): Enterprise Dispatch Management System Security and Privacy 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.*
Computer Aided Dispatch System	The CAD is used in daily operations to manage emergency and hazard incidents and enable real-time responses to public and employee safety incidents in a safe and efficient manner consistent with national and department standards. Records interface to SLES, and IMARS.	Yes	All PII data elements indicated in Section 2.A. below.
Dispatch Console (DC)	Provides enhanced radio and voice over internet protocol for dispatch centers to communication with LEOs in the field.	Yes	All PII data elements indicated in Section 2.A. below.
911 Recorder (911)	Records all LE and dispatch radio and telephone traffic.	Yes	All PII data elements indicated in Section 2.A. below.
License Plate Reader (LPR)	Scan license plates and identify associated current law enforcement issues for awareness or action.	Yes	Video and photograph of vehicle and license plate, vehicle location, date, and time and a status indicator identifying if there is law enforcement or public safety activity of interest associated with the license plate.

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

☒ Yes
The records are covered under DOI-10, Incident Management, Analysis and Reporting System (IMARS), published June 3, 2014, 79 FR 31974, modification published September 7, 2021, 86 FR 50156.

☐ 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
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Disability Information
☒ Child or Dependent Information
☒ Law Enforcement
☒ Military Status/Service
☒ Mailing/Home Address
☒ Driver's License
☒ Social Security Number (SSN)
☒ Personal Cell Number
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Marital Status
☒ Home Telephone Number
☒ Other Names Used
☒ Truncated SSN
☒ Emergency Contact
☒ Place of Birth
☒ Race/Ethnicity
☒ Other
CAD contains law enforcement information and may also include the following information from individuals: License Plate Numbers; Vehicle Identification Number (VIN); vessel registration numbers; Passport Numbers; Alien Registration Numbers; State Identification Numbers (SID); Criminal History Record Information (CHRI); physical description of the individual including any physical attributes; officer's information; and information on the dispatcher entering or accessing the data. These individuals are typically persons believed to be involved in or related to a particular incident, such as suspects, victims, witnesses, participants, employees, and building occupants and visitors. The type of information collected about these individuals varies depending on the type of incident that occurred, but basic identifying information (such as name and contact information) is usually collected at a minimum.

The LPR captures video and still photographs of the vehicle and license plate which may include persons or other information, e.g., location background information, bumper stickers. The location (e.g., main entrance, fee station, exit, camera location), date and time are also captured with the video and photographs. A status indicator is associated to the license plate to identify whether there is LE or public safety activity of interest associated with the license plate (e.g., BOLO, Amber alert, warrant, hot list).

The photos collected may contain images of victims, suspects, or other areas of interests to aid in the recording, documentation, or investigation of the incident.

If the SSN is collected from an individual, it is used to identify the individual and to perform record checks in Federal, State, Tribal and local government law enforcement information systems such as the SLES and NCIC. Contextual information about the individual in relationship to the incident or offense may also be collected, some of which may be sensitive. For example, for persons injured in a slip and fall, the systems may record the type of injury suffered (e.g., broken leg) and the details of the event itself. For criminal activity, the systems may reflect the relationship of the individual to the crime (e.g., victim, witness, suspect), the nature and details of the crime (e.g., assault), and any personal property that was damaged or stolen.

Name, username, email address and password collected for government employee and contractor users of the EDMS for the purposes of account access and permissions management.

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*

PII may also be collected from international law enforcement agencies through SLES and NCIC interfaces. Individual law enforcement jurisdictions determine the data to make available.

Information may also be obtained from publicly available sources, such as web sites, newspapers, and press releases. Documents and other artifacts, such as audio or images, collected from publicly available sources that may contain PII are not appended to EDMS dispatch transaction records, though links to the information may be recorded. Building floor plans may be entered in the EDMS for the purpose of assisting dispatch center staff and LEOs in responding to fire and security calls.

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: *Describe*

Information is collected from telephone, text, email, and face-to-face contact between individuals and LEOs and dispatch center staff.

PII is collected in search results returned through SLES and NCIC interface(s). Individual jurisdictions may determine the data to make available for search or import, but search criteria are generally limited to name, sex, date of birth, state, and driver's license information. Soundex search (matching by sound despite minor spelling differences) is available for data elements, such as name.

Information may also be obtained from publicly available sources, such as web sites, newspapers, and press releases. Documents and other artifacts, such as audio or images, collected from publicly available sources that may contain PII are not appended to EDMS dispatch transaction records, though links to the information may be recorded. Building floor plans may be entered in the EDMS for the purpose of assisting dispatch center staff and LEOs in responding to fire and security calls.

The LPRs capture video along with date, time and location data from cameras posted within and at entrance and egress points from the park or office. Still photographs are derived from the video captured. A status indicator is associated to the license plate to identify whether there is LE or public safety activity of interest associated with the license plate based on information from the SLES or an internal law enforcement list (e.g., hot list, BOLO). No additional PII is recorded in the LPR subsystem from the SLES interface. For license plates identified to be of interest, dispatch personnel may record

activity in the CAD subsystem and capture related PII data returned through the SLES interface.

A uni-directional data interface uploads data to IMARS using the IMARS application programming interface (API). The API sets a standard process of how third-party applications submit data to IMARS. The API data is encrypted from end to end. The user's credentials are submitted to the API to perform an action and based on his/her role it will be executed in the IMARS report system. Data is not downloaded from the IMARS system.

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

The intended use of the information collected is to complete criminal investigations conducted by commissioned Law Enforcement staff, increase the efficiency of emergency dispatch and response, record, and document incidents inside the National Parks and to increase the safety for both park staff and visitors. 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:

The EDMS shares data with the DOI IMARS system which is accessible by other NPS law enforcement and criminal justice personnel, and subject to IMARS security protocols for data entry and accuracy. This data will be used to aid LEOs in criminal investigations. PII will only be shared with criminal justice personnel to assist with investigations and incidents. PII may be shared with between NPS park unit(s) and office(s) related to the investigation, apprehension, and the possible arrest and/or conviction of crimes committed on DOI properties and/or against DOI or employee, volunteers, contractors, concessioners, and visitors.

☒ Other Bureaus/Offices:

The EDMS shares data with the DOI IMARS system which is accessible by other NPS law enforcement and criminal justice personnel, and subject to IMARS security protocols for data entry and accuracy. PII may be shared with DOI bureaus and offices related to the investigation, apprehension, and the possible arrest and/or conviction of crimes

committed on DOI properties and/or against DOI or employee, volunteers, contractors, concessioners, and visitors.

The IMARS Privacy Impact Assessment is available for review at Privacy Impact Assessments | U.S. Department of the Interior (doi.gov). NPS maintains a memorandum of understanding with DOI to cover all interfaces between IMARS and the NPS General Support System and computer-aided dispatch systems.

☒ Other Federal Agencies:

PII could potentially be shared with other Federal agencies related to the investigation, apprehension, and the possible arrest and/or conviction of crimes committed on NPS properties. Information may also be shared between Law Enforcement and other Federal agencies. Information from this system is primarily shared with the United States Department of Justice and its subordinate agencies.

EDMS subsystems maintain interconnection agreements with NCIC. The NCIC Privacy Impact Assessment is available for review at https://www.fbi.gov/file-repository/pia-ncic.pdf/view.

U.S. Park Police (USPP) CAD will share incident data with the Presidio Trust. This data will include LEO state identification number and incident location information. No PII on members of the public will be shared. This information will be used by Presidio Trust for statistical analysis and data mapping purposes only.

☒ Tribal, State or Local Agencies:

The EDMS shares data with the DOI IMARS system which is accessible by Tribal law enforcement and criminal justice personnel, and subject to IMARS security protocols for data entry and accuracy. PII could potentially be shared with Tribal agencies related to the investigation, apprehension, and the possible arrest and/or conviction of crimes committed on NPS properties. EDMS maintain interconnection agreements with the SLES to support interface related controls.

☒ Contractor:

NPS may contract with other commercial organizations to provide application development, configuration and operations, and maintenance of EDMS components or specific subsystems. Contractor staff will be required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the EDMS System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system. EDMS undergoes a security assessment by a third-party assessment organization each year. Contractor's staff access must be initiated, authorized, and monitored by NPS personnel.

☒ Other Third-Party Sources:

EDMS may share information with the news media and the public in support of law enforcement activities, including obtaining public assistance with identifying and locating criminal suspects and lost or missing individuals, providing the public with alerts about dangerous individuals, or protecting the integrity of DOI, NPS, or any DOI employee acting in his or her official capacity.

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

☒ Yes:

Individuals contacting the dispatch center by phone, text or email have the option to decline to provide PII. An anonymous tip line is also available for this purpose. However, this may result in delay in or inability of law enforcement or search and rescue response.

Information may be provided to LEOs for relay to the dispatch center and entry to the EDMS. Individuals may decline to provide PII; however, in some instances the individual in question may be required by law to provide the information, such as when the information collected is the result of criminal investigations conducted by commissioned park Law Enforcement staff, and failure to provide information may result in legal consequences and/or may result in delay or inability of execution of law enforcement or search and rescue operations.

Data collected from national and state records systems, NCIC, and SLES are subject to the collection procedures associated with those systems. NPS does not filter or change these records when interfacing with or storing copies of the records. Individuals should consult privacy notices and assessments published by those system owners for options and impact of decline to provide information.

LPR camera locations are posted to notify individuals that privacy data is collected and that there should be no expectation of privacy on Federal property. Individuals may avoid collection of their data by avoiding park units or camera locations.

Individuals will not have an opportunity to consent to specific uses of their PII because any video and still images of individuals are captured in support of authorized law enforcement or national security activities. PII will not be retained, used or disseminated unless there is a legal reporting requirement, retention of the information is necessary to an authorized mission, the information is maintained in a Privacy Act system of records

or retention is required by any other applicable law or regulation. Allowing an individual to consent to the collection, use, dissemination, and maintenance of information collected for law enforcement purposes would compromise operations and would interfere with DOI's mission.

PII is collected from NPS employees and contractors who must use the system to perform the duties of their employee, contract, or volunteer position. NPS employees and contractors may decline to provide information during the onboarding process; however, this may result in reassignment to another position or a withdrawal of the offer of employment.

☐ No:

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

☐ Privacy Act Statement

☒ Privacy Notice:

Notice is provided through the publication of this PIA and the DOI-10, Investigation Management, Analysis and Reporting System SORN, which is available on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

☒ Other:

Formal written notice is not provided to individuals at the point of collection of this information because of the law enforcement context in which it is collected. In some instances, providing notice to individuals whose information is being collected would interfere with NPS's ability to carry out its law enforcement mission by potentially frustrating the confidential nature of its investigations, methods, or sources. Notice is provided to the individual when the information is collected directly from the individual during or after arrest through the reading of Miranda rights. When information is obtained through witnesses, no specific form of notice is provided.

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 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 activities. Audio and image artifacts are not uploaded to the EDMS.

☐ None

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

EDMS allows dispatchers to search based on unique search criteria such as: first name, last name, location of the previous CAD records, including wildcard searches (partial last name followed by %). Inquires can use a wildcard or partial numbers, words, and phrases. Typical searches will be on persons' names, vessel registration numbers, vehicle license plates numbers, types of incidents, case numbers, CAD event numbers and incidents by locations.

Data is retrieved by name, SSN, home address, work address, phone numbers, emergency contact information, driver's license or other forms of ID, ethnicity and race, date of birth, gender, physical description of the individual including any physical attributes, and incident data.

Reports may be produced on government employee and contractor users for purposes of account and incident management. Reports may be retrieved by name, username, email, or LEO identifier.

I. Will reports be produced on individuals?

☒ Yes

The EDMS can produce reports on the number of incidents, incidents by location, individuals entered into the system, vehicles and boats entered into the system, and user inquiries. These reports will be used to increase the safety of our Law Enforcement staff and that of our responding emergency personnel, as well as court related information and yearly statistical data. The reports generated by Presidio Trust from the USPP CAD contains only information for statistical and data mapping purposes. This report does not contain PII on members of the public.

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.

Reports may be produced on government employee and contractor users for purposes of account and incident management. All reports are access-controlled, and only government employee users with the appropriate need-to-know will be given access to the reports.

☐ No

Section 3. Attributes of System Data

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

For members of the public, NPS relies on the accuracy of the information provided by the individuals. LPR, 911, and DC records are automatically recorded and assumed to be accurate at time of entry.

Validation rules in CAD systems prevent users from submitting information not conforming to data definitions. The EDMS CAD subsystems provide basic data accuracy checking. The CAD subsystems have an internal check system that ensures that incorrectly formatted data cannot be entered. The individual collecting the data will verify the accuracy of data collected per the defined policy and procedures of each participating organization. Supervisors will also review data for accuracy.

The EDMS retrieves its data relating to individuals from the NCIC database. NCIC policies require the inquiring agency to contact the entering agency to verify the information is accurate and up to date. Once the record is confirmed, the inquiring agency may act to arrest a fugitive, return a missing person, charge a subject with violation of a protection order, or recover stolen property.

In addition to the steps listed above, additional NCIC policies include security measures to ensure the accuracy, privacy and integrity of the data. For instance, the information passing through the network is encrypted to prevent unauthorized access. Each user of the system is authenticated to ensure proper levels of access for every transaction. To further ascertain and verify the accuracy and integrity of the data, each agency must periodically validate its records. Agencies also must undergo periodic audits to ensure data quality and adherence to all security provisions. Additionally, any individual with access to the NCIC database must complete a yearly certification through the Criminal Justice Information Services (CJIS) office.

B. How will data be checked for completeness?

For members of the public, NPS relies on the completeness of the information provided by the individuals. LPR, 911, and DC records are automatically recorded and assumed to be complete at time of entry.

Validation rules in CAD prevent CAD users from submitting information not conforming to data definitions. Dispatch centers have multiple policies in place to ensure the completeness of data. Initially, information is verified between the Law Enforcement Rangers and Dispatch operators utilizing the system.

Specific information is required to access records in the NCIC system. Dispatch operators gather this information from LEOs. The EDMS will then process the information provided. The Dispatch operator then confirms the information with the LEO. The LEO then verifies the information is accurately entered into IMARS through the EDMS.

Additionally, the Dispatch supervisor ensure that Dispatch operators are completing all required and relevant fields and verify the system is being utilized properly.

The EDMS itself has multiple accuracy and completeness checks embedded in the programming. This includes error messaging for incorrectly formatted data and failure to provide information in required fields.

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

Search results from other systems are historical data and are captured as of a point in time. LPR, 911, and DC records are automatically recorded. These records are not updated.

CAD records are updated by dispatch center staff and by LEOs based on user permissions assigned and investigation status and results. Changes are logged by the system. The individual collecting the data and entering the data into CAD will verify the accuracy of data collected pursuant to policy and procedures defined by NPS. Supervisors will also periodically review data for currency.

Data changes are also verified for accuracy through the use of data intelligence analysis tools, research, investigation techniques and review by IMARS and CAD users and supervisors.

CAD users and dispatch supervisors are responsible for maintaining current information in the user accounts, and supervisors are responsible for notifying the system administrator within 24 hours of any account termination required.

D. What are the retention periods for data in the system?

EDMS records are retained in accordance with the National Park Service Records Schedule, Protection and Safety (Item 2), which has been approved by the National Archives and Records Administration (Job No. Nl-79-0802). The disposition for significant protection and safety case files that document incidents, investigations, or activities that a) cause significant or permanent damage to, or loss of, a cultural or natural resource with great monetary, cultural, scientific, or historical value; b) "first of kind" events that establish precedents; c) subject of widespread media attention or

Congressional scrutiny; and /or d) substantiated Native American Graves Protection and Repatriation Act (NAGPRA), Archaeological Resources Protection Act (ARPA), and Indian Arts and Crafts Board (IACB) claims are permanent records and are transferred annually to the National Archives when 3 years old. The disposition for major protection and safety case files that document major incidents, investigation, or activities that a) are generally criminal in nature; and/or b) are unsubstantiated NAPGRA, ARPA, and IACB claims; and c) do not meet the permanent record standard is temporary and records are destroyed/deleted 25 years after closure. The disposition for minor protection and safety case files that document emergency management and search and rescue or minor incidents, investigation or activities is temporary, and records are destroyed/deleted 7 years after closure. The disposition for routine protection and safety case files is temporary and records are destroyed/deleted 3 years after closure.

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?

After the retention period has passed, temporary records are disposed of in accordance with the applicable records schedule and DOI policy. Disposition methods include pulping, shredding, erasing and degaussing in accordance with Departmental policy. Permanent records that are no longer active or needed for agency use will be transferred to the National Archives for permanent retention in accordance with NARA guidelines.

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 EDMS due to the amount of sensitive PII that may be captured and used or maintained for law enforcement purposes. The risks are mitigated by controls implemented to limit unauthorized exposure of PII. EDMS 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 access, and system access is based on least privilege access and role-based access controls.

Potential privacy risks include the interception of data in transit entering the EDMS through the NCIC, and SLES interfaces, and data leaving the EDMS and entering

IMARS. These risks are mitigated by utilizing secure Virtual Private Networks (VPN) and data encryption and transmission. Data located in the EDMS itself is protected by the NPS firewall, two-factor authentication for computer and software use, Active Directory permission groups, and secured facility entry on federal property. The EDMS produces audit logs for every action the user takes within the software. The logs will be regularly reviewed by authorized park staff in addition to federal and state officials. The EDMS submits information to IMARS via scheduled transmissions of encrypted data and users cannot access IMARS through the EDMS.

Privacy risks exist with data sharing with other law enforcement organizations related to the unauthorized sharing, data integrity or loss of data. EDMS supports law enforcement activities at NPS 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 NPS lands and/or against NPS personnel. The system provides dispatch management and law enforcement officials audio and video recording capability to document dispatcher/officer-citizen encounters while engaged in dispatch management and patrol functions, which are used in law enforcement activities on lands/areas governed by the NPS as well as tribal lands. There is a risk of unauthorized sharing or loss of data or data integrity related to external sharing of data with other Federal, state, Tribal, and local law enforcement, security, and emergency services organizations. PII may be 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.

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

These devices may capture audio and images of persons, places and events occurring in real time as part of ongoing dispatch management and law enforcement operations, such as identifying persons involved in potential criminal activity or persons or vehicles entering or existing NPS properties. Some devices may capture metadata such as audio, images or recordings which provide the time, location, and date of the event. Images or 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 than is necessary to accomplish law enforcement objectives. The devices are used by authorized law enforcement officials to support law enforcement activities, 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.

There is the risk that the use of the audio recording devices may restrict First Amendment protected activities like freedom of speech or association. Audio and images associated with First Amendment demonstrations will be used for the sole purpose of identifying and recording the presence of individual participants engaged in unlawful conduct. First Amendment demonstrations may be recorded 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 that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled. System administrators periodically review audit logs to prevent unauthorized monitoring. Users are required to accept rules of behavior when using the system. All users must have an account in the system and user authentication protocols are enforced based on the user's role and permissions, i.e., personal identity verification (PIV) cards, two factor authentication, two step verification. Government employees will be required to use two-factor authentication. Government Users will be authorized for their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created in EDMS. Government Users will authenticate to EDMS using the applicable agency identity provider (e.g., Active Directory Federated Services for DOI) and their DOI- issued PIV card.

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which will be referenced in the System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. A very limited number of system administrators may have limited access to volunteer profiles for support purposes only (e.g., password reset, login monitoring, incident response, etc.).

There is a risk that individuals may not know why their information is being collected, how it will be used or who it will be shared with during and following the application, partnership, and reporting processes. The public is also provided notice of the collection, uses and sharing of information through publication of this PIA and the applicable system of records notices.

There may be a risk associated with hosting the system with an on-premises data center. A formal Assessment and Authorization for issuance of an authority to operate will be/has been conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system has been rated as moderate, requiring management, operational, and technical controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. As part of continuous monitoring, continual auditing will occur to identify and respond to potential impacts to PII information.

Contractor support personnel require access to the system to provide support and maintenance. This maintenance is critical to protecting the system and any PII contained in the system. Contractor's staff access must be initiated, authorized, and actively monitored by NPS personnel through the session. Contractor must also have userid and password permission monitored by LEO and dispatch supervisor staff. Contractor activity is also logged by the system. NPS contractor staff are required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in published procedures.

In addition, Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that information may be used outside the scope of the purpose for which it was collected. Dispatch management and law enforcement personnel with access to data and recorded material will be subject to strict DOI policy, NPS policy, and Privacy Act standards. These 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 dispatch or law enforcement operations, 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 data, images and recordings does not exceed approved periods necessary for law enforcement purposes. DOI restricts the maintenance of images or recordings 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. 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 will be 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 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 license plate readers, and the CCTV Policy Statements posted on National Park websites. Case law has established that cameras in a public area where there is no reasonable expectation of privacy and do not violate the law.

There is a risk of proactive release of audio or visual information and/or that PII may not be redacted properly and that individuals identified may experience identification, misidentification, harm, inconvenience, embarrassment. Proactive release may occur as deemed necessary by DOI or NPS to prevent harm to the public or to DOI, NPS or NPS personnel or contractors. Individuals have the opportunity to correct records through the redress process provided on the DOI Privacy Act Requests website at https://www.doi.gov/privacy/privacy-act-requests.

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.

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 intended use of the information collected by the EDMS is both relevant and necessary to the purpose for which the system is being designed. The information is needed to accomplish the specific purposes of the system and will be used by Law Enforcement and Dispatch staff in daily operations to receive and facilitate emergency response to public and employee safety incidents in addition to assisting Law Enforcement staff in completing criminal investigations. Organization of historical data and the ability to immediately maintain and recall that information along with access to the related information systems previously mentioned will directly result in added safety

to park LESES and non-LESES staff, as well as the general public and park visitors. This corresponds directly to the underlying mission of the park.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

Not applicable. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

The EDMS allows Law Enforcement staff to retrieve data from the NCIC, and SLES databases; however, search results are not consolidated with EDMS incident records.

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

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

LEOs or emergency responders may request and receive information by contacting the dispatch center operators.

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

User access to the data is limited to commissioned LEOs and Dispatch operators whose official duties require such access. To implement the parks intended use of the EDMS, LEOs and Dispatch operators will have full use of the CAD software system itself, minus activity or audit logs, which will be strictly limited to approved personnel. Security measures such as a review of official duties, Active Directory permission groups, network user accounts, expiring network user account passwords, and PIV cards will establish access levels for different types of users.

Access to the NCIC and IMARS is determined by assigned official duties.
Access to national and state criminal databases will remain at the current level for individuals with previously approved access. Restriction levels are set to the highest possible level that allows for the performance of required tasks.

System administrators, such as approved DOI and NPS IT staff, will have access to the CAD software itself for software maintenance purposes, but will not have access to the related Law Enforcement systems (NCIC and IMARS) outside of the EDMS. No other staff will have access to 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, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974, 5 U.S.C. 552a, and applicable agency regulations.

Contractor employees interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. Information security and role-based privacy and security training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to sensitive data.

☐ 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

☒ No

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

☒ Yes

CAD will not be used for monitoring members of the public. Members of the public are not users of the system.

Monitoring will primarily target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

EDMS systems not intended for monitoring users; however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit, including identity verification method, action attempted and the status of the attempt, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

☐ No

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

The EDMS system can record every action in the system. This includes which user is logged into the system and any invalid log in attempts, every piece of data the user accesses, all inquiries and returns for any data requested or searched for by the user, any updates or deletions, and before and after states for all pieces of data. Every log is timestamped and associated to the user performing the edit or request.

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

Due to the sensitive nature of the information collected in the EDMS, controls are in place to ensure that only authorized personnel can monitor use of the system. Access to monitoring the system will be limited to approved Law Enforcement staff, Dispatch operators, and system administrators such as approved DOI and NPS IT staff.

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance. All access to the system, including the generation of reports, creates an audit log entry. Periodic audits will be performed by the Information Systems Security Officer.

To ensure access is limited the park will implement a Standard Operating Procedure (SOP) with specific use instructions for all staff with access to the system. The EDMS also records requests for logs and which user is responsible for changes. User groups within the EDMS will have tiered permissions so that only specific individuals have access to monitor system use. Contractor staff must be actively monitored by an NPS system administrator during any system access.

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.

☒ 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. *Describe*

(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 serves as the EDMS Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in EDMS. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with

Federal laws and policies for the data managed and stored within EDMS, in consultation with NPS 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 EDMS Information System Owner and EDMS Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.