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: Department of the Interior Emergency Notification System (DOI ENS)

Bureau/Office: Office of the Secretary/Office of Emergency Management
Date: July 13, 2021

Point of Contact:
Name: Danna Mingo
Title: DOI Departmental Offices Associate Privacy Officer
Email: OS_privacy@ios.doi.gov
Phone: (202) 208-3368
Address: 1849 C Street, NW, Room 7112, Washington, D.C. 20240

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/Federal Contractor and/or State Partners
☒ Volunteers
☐ All

☐ No:

B. What is the purpose of the system?

The Department of the Interior Emergency Notification System (DOI ENS) is an emergency notification and employee accountability cloud-based application that provides organizations with the ability to quickly send critical information to recipients. It is the DOI ENS that is replacing the Send Word Now ENS, the Department has been using. The system collects, modifies, updates, and safeguards contact information for emergency situations, including natural, environmental, or austere weather conditions affecting the Department of the Interior

(DOI) mission or function, emergency contacts, and agency continuity of operations. In emergency situations where active involvement of the vendor is necessary due to the loss of DOI primary and normal means of communication, the system may be used to facilitate and transfer communications between agency leaders in support of continuity of operations and provide alerts and other response needs as determined by DOI.

The system is centrally managed by the DOI Office of Emergency Management (OEM) and may be used by DOI bureaus and offices, including National Park Service, Bureau of Land Management, U.S. Fish and Wildlife Service, Bureau of Indian Affairs, Bureau of Reclamation, Bureau of Ocean Energy Management, Bureau of Safety and Environmental Enforcement, Office of Natural Resources Revenue, U.S. Geological Survey, Bureau of Indian Education, Office of Surface Mining, and the Office of the Secretary. The system may be used in abnormal operations as defined by the Office of Personnel Management. Examples the system uses may include notifications of response level or alert declaration, continuity events or activities, building or facility closure or access issues, weather events (severe storms, flooding, etc.), security alerts/threats/incidents, exercise messaging, safety messaging, and communications drills.

The DOI ENS is provided by Everbridge which is a Software as a Service (SaaS) cloud service provider located in the United States. Everbridge is FedRAMP authorized.

C. What is the legal authority?

5 U.S.C. 301; 44 U.S.C. 3101; 6 U.S.C. 101 et seq., Homeland Security Act of 2002; 50 U.S.C. App. 2062, The Defense Production Act of 1950, as amended; 31 U.S.C. §§ 1535-1536, Economy Act; 50 U.S.C. §§ 1601-1651; 42 U.S.C. 247d and 300hh, The Public Health Security and Bio-terrorism Preparedness and Response Act of 2002; Pub. L. 106-390, Robert T. Stafford Disaster Relief and Emergency Assistance Act; Executive Order 12656, Assignment of National Security and Emergency Preparedness Responsibilities; Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Operations; Federal Continuity Directive - 1, Federal Executive Branch National Continuity Program and Requirements; Federal Property Management Regulation (FPMR) 101-20.103-4, Occupant Emergency Program; Homeland Security Presidential Directive 20, National Continuity Policy; 900 Departmental Manual Chapters 1-5, Emergency Management Program; and Department of the Interior Continuity of Operations Plan.

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: System Name Change

E. Is this information system registered in CSAM?

☒ Yes:

CSAM ID: 2564
UII Code: 010-000001989
SSP Name: DOI Emergency Notification System (ENS)

☐ 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.*
None			

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

☒ Yes:

DOI-58, Employee Administrative Records - 64 FR 19384 (April 20, 1999); modification published 73 FR 8342 (February 13, 2008) and DOI-85, Payroll, Attendance, Retirement, and Leave Records - 83 FR 34156 (July 19, 2018). Some information in this system may be covered under OPM/GOVT-1, General Personnel Records, 77 FR 73694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015).

☐ 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 ☒ Personal Cell Telephone Number ☒ Spouse Information
☒ Personal Email Address ☒ Home Telephone Number ☒ Mailing/Home Address
☒ Other:

The DOI ENS may also contain contact information of non-Federal entities who are partners with DOI on an opt in basis to include personal email addresses and personal phone numbers, employee job title, work email address, office phone number, work cell phone number, organization code, group name and membership for roles in emergency management groups, and username. Information may also include spouse contact information such as phone numbers, email.

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:

Information may be extracted from DOI employee records from DOIAccess and Active Directory (AD). Data may also be manually added to the system or updated by authorized Bureau/Office managers or by the employee through a Member portal that leverages official email addresses in AD or Single Sign-On IDs (SSO-IDs) to review their contact record and make the necessary updates. This request may be initiated by Bureau/Office designated administrator. Data may also be added by non-Federal entities and DOI partners on an opt in basis. An automated update process is currently in development for each bureau and office.

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:

Information may be collected from DOI employee records within DOIAccess and Active Directory.

☒ Other:

Non-Federal entities and DOI partners may opt in to provide personal contact information if the Bureau/Office invites the non-Federal entities and DOI partners to update their contact information.

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

The PII collected in the contact records is necessary for the DOI Continuity of Operations (COOP), Emergency Management (EM), Employee Accountability, and Occupant Emergency Programs to have multiple methods of contacting EROs, Crisis Management Teams, DOI employees, and non-Federal entities and DOI partners during an emergency to ensure emergency contacts and operations sustain a continuity of operations. This information will be used for emergency alerts, safety messaging, and other notifications to DOI employees and non-Federal entities and DOI partners who are on or off duty regarding incidents, emergencies, office closures, tests, and/or exercises.

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

☒ Within the Bureau/Office:

Contact information is provided to the Office of the Secretary (OS) COOP Team members or EM Coordinators to verify members on the contact lists.

☒ Other Bureaus/Offices:

The DOI ENS is being utilized throughout bureaus and contact lists are managed at the lowest unit level possible, in most cases. Distribution lists may be shared with authorized personnel (based on their roles in the DOI ENS) for the purposes of employee accountability, safety messaging, recall, and other contingency operations.

☐ Other Federal Agencies
☐ Tribal, State or Local Agencies
☒ Contractor:

The Office of the Chief Information Office (OCIO) contract support staff have access to the records in order to determine causes related issues with data uploads or communications. The staff analyzes the message history and logs to determine where a failure may have occurred, such as an incorrect phone number or email address. DOI/OCIO contractors also have access to records in order to provide the support to resolve issues between AD and DOIAccess.

☐ Other Third-Party Sources

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

☒ Yes:

Individuals may decline to provide the contact information; however, the individual will not receive the emergency notifications from DOI. During a routine self-update, individuals have the option to provide all, some, or none of the non-work contact information. As a member of the DOI emergency management community, each contact must ensure their information is current to perform their role as an Emergency Response Official (ERO).

Non-Federal entities and DOI partners have the option to provide all, some, or none of their personal contact information.

☐ No:

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

☒ Privacy Act Statement:

A Privacy Act Statement will be included in the Member Portal/email request. In some cases, a privacy notice may be added to phone trees or emergency contact lists used in parallel with DOI ENS and as an alternate if DOI ENS is unavailable. Individuals are also provided notice through the publication of this privacy impact assessment and related assessments, and applicable DOI system of records notices, DOI-58 and DOI-85.

☐ Privacy Notice
☐ Other
☐ None

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

Data is retrieved manually by an administrator or other privileged user or message sender. Contact record information is retrieved by last name, group name or membership. Group membership is identified in group membership reports generated manually or programmed.

I. Will reports be produced on individuals?

☒ Yes:

DOI ENS managers have the ability to produce reports on individuals (names, contact information, etc.) and their response to messages when submitted. This capability is limited based on roles within the system those that have a need for this capability. Reports from DOI ENS regarding contact responses to alerts, message history, receipt of emergency notifications, and participation status are used for employee accountability. Reports may be generated to determine the effectiveness of emergency response, exercises, or contingency which will be shared with authorized personnel at bureaus/offices in order to provide feedback and corrective actions.

☐ No

Section 3. Attributes of System Data

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

Bureau/Office authorized managers vet the extracted data and identify any records that should not be uploaded. Updates to the records can be manually entered by the authorized managers or by the employee through the portal or email request to review their contact record and make the necessary updates. This request is initiated by Bureau/Office authorized managers with access to the DOI ENS. Contact records from AD will be uploaded on a regular schedule to ensure new employees are added to the DOI ENS and departed (retired, left DOI, etc.) are removed from the system via automatable secure file transfer or Web Services API. An email update request is sent to employees with instructions on how to update contact records to ensure accuracy of emergency management contact information.

B. How will data be checked for completeness?

The contact information is checked for completeness during the DOI ENS alert notification for events such as fire drills, shelter-in-place, building evacuations, National Level Exercises, and office closures. If the message history for the alert for each contact indicates the message was not received, the contact information such as email address, phone numbers, and text message will be manually checked to confirm the information is correct or needs to be updated.

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

Individuals are sent the self-update email requests regularly by their Bureau/Office authorized managers. Account administrators, data owners, units, groups, or office managers using the account are responsible for keeping the data in their accounts current. To accomplish this task, the system supports a number of data maintenance methods which include direct entry, a flat file (csv, xls, xlsx) import process, a batch extensible markup language file of contact data that is transmitted via an automatable secure file transfer, and a Web Services API using a simple object access control connection. All data maintenance methods used require administrative authentication.

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

Contact records are maintained under the DOI Departmental Records Schedule 1 - DAA-0048-2013-0001-0003, Administration Records of Specific Temporary Value, which was approved by the National Archives and Records Administration (NARA). The disposition is temporary. Records are cut off when the object or subject of the record is removed or discontinued, and records are destroyed when no longer needed.

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

The DOI Emergency Notification System uses software for data deletion or destruction that complies with the U.S. Department of Defense 5220.22-m standards. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records. Disposition procedures are outlined in the DOI ENS Information Security Policy. Disposition occurs after authorization from the appropriate Records Officer using the DI 1941 form and instructions.

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 are risks to the privacy of individuals due to the PII contained in the system related to individual's work phone number, home phone number, work and personal cell phone numbers, and work or personal email addresses. These risks are mitigated by a combination of administrative, physical and technical controls. The contact information is used to communicate with COOP, emergency management personnel, DOI employees, non-Federal entities and DOI partners, and individuals with occupant emergency responsibilities. These individuals must be reachable by several methods. In addition, group email lists need to be current. During COOP training, individuals are informed that their contact information must be current in the system.

Everbridge is a Software as a Service (SaaS) cloud service provider located in the United States. Everbridge is FedRAMP Authorized. The DOI ENS has a Moderate system security categorization based upon the type of data and the requirement for security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system in accordance with National Institute of Standards and Technology (NIST) standards and FIPS 199, and the Federal Information Security Modernization Act (FISMA). A system security plan was developed for the Department of the Interior ENS to ensure appropriate security controls were implemented to safeguard DOI information transmitted, processed or stored, including access controls, password management, firewalls, segregation of duties, and encryption of database, media and communications. This application uses the principle of least privilege access for authorized users to perform duties, and government information is managed and safeguarded in accordance with FISMA, Office of Management and Budget policies, NIST standards, and DOI security and privacy policies. The DOI ENS is subject to monitoring consistent with applicable security and privacy laws, regulations, OMB policy, and DOI policies and procedures.

Data will be used for emergency alerts and notifications of DOI employees and non-Federal entities and DOI partners on incidents, emergencies, safety messages, tests and/or exercises. Bureau/Office authorized managers and bureau/office EM Coordinators notify OEM when a member should be deleted. Authorized users will immediately delete the individual's record and from groups. An authorized user may confirm the record has been deleted in DOI ENS. After the termination of a client contract or service, a legal review will be completed on the contract to determine further actions necessary for this data and whether the data will be destroyed, retained, or returned.

The use of DOI information and information technology (IT) systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access; activities performed using a system administrator's identification; and activities that could modify, bypass, or negate the system's security controls. Audit logs will be reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI Rules of Behavior.

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 application is relevant and necessary for collecting, modifying and safeguarding contact information for emergency situations affecting the DOI mission or function, employees, emergency contacts, and agency continuity of operations.

☐ 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?

The 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.

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?

Bureau/Office authorized managers and bureau/office EM Coordinators identify who is authorized to access the system. Bureau/Office authorized managers and bureau/office EM Coordinators who may initiate alerts for closures, testing, drills, and emergencies. Bureau/Office authorized managers and bureau/office EM Coordinators have rights to create users, input or initiate updates to contact information and generate roster reports. Bureau/Office EM Coordinators are responsible for rebuilding DOI operations at different locations when operations have been incapacitated. Bureau/Office authorized managers and bureau/office EM Coordinators can assign access rights to view or edit records.

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.

Privacy Act contract clauses were included in the ATT/Everbridge contract.
- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.239-1 Privacy or Security Safeguards (Aug 1996)

☐ 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.

The system contains a Message History with a Summary, Delivery Status, Recipient Status, and Report. The Reports and Audit Trail is a reporting tool with the ability to generate reports and view when groups or contacts were created or modified, the username of the individual that changed the record, and the date and time the record was updated. Information in the history and audit log may include contact person responses, date/time, mode of contact such as Short Message Service, cell, or email. The system logs all changes to customer accounts for auditing purposes and are only accessed by administrative/manager staff to track the date, time and action. The auditing feature does not allow for the application to be used or changed without administrative notification.

☐ No

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

Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and time-stamp) for auditing purposes.

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

Access to this program is only provided to the necessary authorized employees and is applied on the principle of least privilege access to allow authorized employees access to the tracking information. Audit features track user activity and the DOI ENS administration system logs all changes to customer accounts for auditing purposes.

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 Director, Office of Emergency Management, is the DOI ENS Information System Owner and the official responsible for oversight and management of the system security controls and the protection of agency information processed and stored in the DOI ENS. The Information System Owner and DOI ENS Privacy Act System Manager, in collaboration with the DOI Senior Management Team, 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 the system. These officials, DOI bureau and office emergency response officials, and authorized DOI ENS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with DOI Bureau and Office Privacy Officers.

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 DOI ENS Information System Owner is responsible for oversight and management of the system security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures. Customer communications are managed through an initial point of contact service model. Customer Support Managers (CSMs) serve as the initial point of contact for assuring the proper use of client data, as well as informing clients of the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. The Customer Support management team will also be involved in this process as necessary.