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: BSEE!Safe Direct Messaging Service
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: July 14, 2022
Point of Contact:
Name: Rowena Dufford
Title: Associate Privacy Officer
Email: privacy@bsee.gov
Phone: (703) 787-1257
Address: 45600 Woodland Road, Sterling VA 20166

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 Department of the Interior (DOI) Bureau of Safety and Environmental Enforcement (BSEE) executes its responsibilities and mission under the statutory authority of the Outer Continental Shelf Lands Act (OCSLA), 43 U.S.C. 1331-1356a. When BSEE has critical safety information to share with offshore oil and gas workers and employees, the Office of Public Affairs (OPA) uses BSEE!Safe Direct Messaging Service to quickly notify them of new safety information posted to BSEE.gov. The information consists of publicly available safety alerts and bulletins. BSEE!Safe collects, modifies, updates and safeguards contact information for offshore oil and gas workers interested in DOI BSEE safety information.

BSEE uses Everbridge to perform BSEE!Safe Direct Messaging Service functions. Individuals voluntarily subscribe or opt-in to receive email or text notifications of newly published safety information posted on BSEE.gov. Subscribers may update their information or preferences at any time, including opting-out of the messaging service.
Everbridge is a cloud-based application that provides organizations with the ability to quickly send critical information to recipients. Everbridge is a FedRAMP authorized (Package ID F1412165928 P-ATO) Software as a Service (SaaS) cloud service provider with all federal government data stored in the United States.

C. What is the legal authority?

The Outer Continental Shelf Lands Act (OCSLA), 43 U.S.C. 1331-1356.

D. Why is this PIA being completed or modified?

☐ 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 Code: 010-000002659; Everbridge Suite SSP v3.7

☐ 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	None	No	N/A

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-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), which may be viewed at https://www.govinfo.gov/content/pkg/FR-2011-07-22/html/2011-18508.htm.

☐ 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 ☒ Personal Email Address
☒ Other: BSEE collects the minimum information necessary to issue safety notifications and manage the subscription service. Individuals signing up to receive safety notifications must setup a BSEE!Safe account by creating a username and password, selecting a security question and providing an answer, and providing their name, organization, and information for their alert preference (email address and/or phone number). Most subscribers provide business-related contact information however, some individuals may choose to provide their personal contact information.

BSEE reviews aggregated subscriber data to evaluate performance and manage notification services. This aggregate data includes the number of opt-in requests, the number of opt-out requests, click rates for messages, and undeliverable messages (bounces).

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

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

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

☐ Paper Format
☒ Email

☒ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems *Describe*
☒ Other: For new subscribers: Individuals will generally opt-in to receive notifications by completing a Web form hosted by Everbridge. However, there may be occasions where individuals call, email, or request BSEE assistance in person to register for the service or update their subscription preferences. BSEE officials ensure that individuals have access to the proper privacy notice when they provide information to the bureau.

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

BSEE uses the information to register new subscribers, manage email and text subscriptions, update subscription preferences, and notify subscribers of newly published safety information posted on BSEE.gov.

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

☒ Within the Bureau/Office: Information is only shared with authorized personnel in BSEE to manage subscriptions and notify subscribers of newly published safety information posted on BSEE.gov.

☒ Other Bureaus/Offices: BSEE generally does not share any of the PII that becomes available to the bureau through the service beyond BSEE OPA. However, there may be unusual circumstances where user interactions potentially indicate criminal activity, a threat to the U.S. Government or the public, or a violation of DOI/BSEE policy. In such instances, BSEE may use information that becomes available through interactions with users of the service to notify the appropriate agency officials or law enforcement organizations.

☐ Other Federal Agencies: BSEE does not routinely share subscriber information with other federal agencies except in cases in which sharing the information is required by law or authorized under the Privacy Act and published routine uses in the DOI-08, Social Networks system of records notice, which may be viewed at: https://www.govinfo.gov/content/pkg/FR-2011-07-22/html/2011-18508.htm.

☐ Tribal, State or Local Agencies:

☒ Contractor: User and subscriber information is hosted by the vendor who may provide operational support for the BSEE!Safe Direct Messaging Service.

☐ 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 voluntarily subscribe to opt-in to receive email or text notifications of newly published safety information posted on BSEE.gov. Subscribers may update their preferences at any time, including opting-out. Individuals are also able to access safety information on BSEE.gov.

☐ No:

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

☒ Privacy Act Statement:

BSEE is requesting this information under 43 U.S.C. 1331-1356 to provide critical safety information related to the Outer Continental Shelf. BSEE offers a free direct messaging service through Everbridge that alerts subscribers of newly published safety alerts and bulletins on BSEE.gov. You may sign up by setting up a BSEE!Safe account and entering your email address and/or cell phone number to receive text and/or email notifications of new BSEE safety alerts or bulletins. Data and messaging rates may apply if you opt to receive text alerts. BSEE will use your information to manage your subscription and will not share your information with third parties for promotional purposes. BSEE does not routinely share subscriber information with external agencies unless required by law, or as authorized under the Privacy Act or the routine uses in DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), which may be viewed at: https://www.govinfo.gov/content/pkg/FR-2011-07-22/html/2011-18508.htm. Providing this information is voluntary, but it is necessary to participate in this messaging service. You may unsubscribe at any time and may access the safety notifications directly on BSEE.gov. You should also review the Everbridge privacy policy to learn how Everbridge uses your information.

☒ Privacy Notice:

Privacy notice is also provided through the publication of both this PIA and the publication of DOI-08, DOI Social Networks SORN.

☐ Other: *Describe each applicable format.*

☐ 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 by last name, email address and cell phone number.

I. Will reports be produced on individuals?

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

BSEE will run reports on subscribers of BSEE!Safe to determine the success of the program. The reports will contain aggregate data that includes the number of opt-in requests, the number of opt-out requests, click rates for messages, and undeliverable messages (bounces) opted into the service. Reports of undeliverable messages will be used to mark subscriber emails for deletion. The BSEE Everbridge administrator or the backups will have an administrative account and 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?

Subscribers voluntarily create BSEE!Safe user accounts and provide their contact information at signup, so BSEE presumes the information to be accurate at the time of collection. In cases in which BSEE provides registration assistance, BSEE OPA will verbally assist subscribers when possible and refer subscribers to Everbridge's Help tab on the sign up page. BSEE OPA will review for undeliverable notifications and responses to email and text messages to verify information accuracy.

B. How will data be checked for completeness?

Information is obtained directly from individuals and is presumed to be complete. In cases in which BSEE provides registration assistance, BSEE OPA will verbally assist subscribers when possible and refer subscribers to Everbridge's Help tab on the sign up page. BSEE OPA will review for undeliverable notifications and responses to email and text messages to verify information completeness.

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

Information received from individuals wishing to subscribe to safety alerts and bulletins is considered to be current at the time of the request. Undeliverable emails or texts will result in the subscriber record's removal from BSEE!Safe.

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 in BSEE!Safe are maintained under Department of the Interior Records Schedule 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 necessary to provide accountability for a specific administrative function or functions, but are not necessary immediately after fulfillment of that purpose, and often cannot be legally retained beyond that task or duty for any substantial length of time. Contact records are cut off when the object or subject of the record is removed or discontinued (e.g., register/list superseded) 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?

Approved disposition methods include erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. A litigation hold for will override any records retention schedule or any other DOI/BSEE policy that may otherwise call for the transfer, disposal, or destruction of the relevant documents until the hold has been removed by an authorized authority.

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.

BSEE!Safe poses a risk to the privacy of subscribers. BSEE expects that most users registering to receive email or text notifications of safety updates posted on http://www.bsee.gov will provide their non-sensitive, business-related contact information. However, there is a greater risk to the privacy of individuals who create user accounts (username, password, and a security question) and provide their personal email addresses and cell phone numbers for safety notifications. BSEE mitigates these privacy risks through a combination of administrative, physical and technical controls.

There is a risk that subscribers will not receive adequate privacy notice. A Privacy Act Statement is provided on the BSEE.gov website at the point of collection to ensure that subscribers receive adequate privacy notice. When subscribers are redirected to the Everbridge page to subscribe to the BSEE!Safe alerts, they are provided with a pop up notice that informs them they are leaving a government website and will be subject to a third party website's privacy policy. The Privacy Act Statement posted on the BSEE.gov website also directs subscribers to review the Everbridge privacy policy for how Everbridge handles information from Web visitors.

Privacy notice is also provided to subscribers through this PIA and the published DOI-08, DOI Social Networks system of records notice. In cases in which BSEE provides registration assistance, BSEE OPA will verbally assist subscribers when possible and refer subscribers to Everbridge's Help tab on the sign up page. BSEE collects only the PII necessary to facilitate and manage subscription services to reduce the risk of collecting more PII than is necessary. In accordance with the Privacy Act Statement, BSEE's use of Everbridge must be solely to issue safety notifications and manage the BSEE!Safe Direct Messaging Service. BSEE users are not permitted to export subscribers' information to use for other purposes. BSEE personnel review and approve proposed safety notification content prior to distribution to prevent the unauthorized disclosure of personal data or internal or proprietary information.

There may be a risk associated with using a cloud service provider to manage the BSEE!Safe Direct Messaging Service. Everbridge is a Software as a Service (SaaS) cloud service provider located in the United States. Everbridge is FedRAMP certified. The BSEE Information Security Branch completed the Assessment and Authorization (A&A) process for Everbridge to be used by the BSEE OPA. The BSEE Authority to Use Everbridge was completed initially and remains current under an ongoing authorization through the continuous monitoring program. Everbridge has a “Moderate” system security categorization. This categorization is based on the type of data and the requirement for security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive information contained in the system in accordance with the National Institute of Standards and Technology (NIST) standards and Federal Information Processing Standards 199, and the Federal Information Security Modernization Act (FISMA). An Everbridge system security plan is on file in the FedRAMP MAX.GOV repository, with a description of all security controls and implementation to safeguard DOI information transmitted, processed or stored, including access controls, password management, firewalls, segregation of duties, and the encryption of database, media and communications.
The BSEE Public Affairs Chief determines which BSEE employees have access to BSEE!Safe and ensures that the access of departing employees is revoked. This application uses the principle of least privilege access for authorized users in BSEE 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. BSEE!Safe is subject to monitoring consistent with applicable security and privacy laws, regulations, OMB policy, and DOI policies and procedures. Data is used to alert subscribers to newly published safety information posted on BSEE.gov. If subscribers contact BSEE and request assistance to unsubscribe or update their contact information, authorized BSEE users will immediately fulfill the requests.

The use of DOI information and information technology (IT) systems is conducted in accordance with the appropriate DOI use policy. The system maintains an audit trail sufficient to reconstruct security relevant events in accordance with applicable DOI guidance. The audit trail includes 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 are 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 system manages the BSEE!Safe Direct Messaging Service for subscribers who choose to opt-in and receive BSEE's safety information alerts.

☐ 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.*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

BSEE!Safe 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. *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: Authorized BSEE personnel will have access to data on a need-to-know basis.

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

Access to data is only provided to a limited number of authorized BSEE personnel and is applied on the principle of least privilege access to allow authorized employees access to the tracking information and, upon the request of subscribers, update subscription preferences and contact information. Audit features track user activity and the Everbridge application administration system logs all changes to customer accounts for auditing purposes. Subscribers have access only to the data they have submitted pertaining to themselves during the subscription sign-up process.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy clauses are included in the contract BSEE has with the vendor. The contract includes the following Privacy Act clauses:

- 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)
- FAR 52.224-3 Privacy Training (Jan 2017)

☐ 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. The system has audit features that allow BSEE to identify and monitor authorized users, as well as any unauthorized user or unauthorized activity. However, the system does not locate or monitor subscribers who elect to receive text and email notifications on safety alerts and bulletins posted to BSEE.gov.

☐ No

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

Only BSEE authorized users who access the system are monitored for authorized activities. Information collected is used to monitor the system administrator and other 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 Everbridge application administration system logs all changes to customer accounts for auditing purposes. All collections of subscriber information are accompanied by a Privacy Act Statement that details the bureau's practices with respect to the collected PII and advises individuals to also read the Everbridge privacy policy; authorized users are aware of these notices and their responsibilities to comply with all relevant federal and DOI policies.

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 BSEE Public Affairs Officer within OPA serves as the Information System Owner for this system and is the official responsible for oversight and management of the program's security controls and the protection of agency information processed and stored by OPA. The Information System Owner, Information System Security Officer, and authorized BSEE!Safe users are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with federal laws and policies for the data managed and stored by OPA, and addressing Privacy Act requests for notification, access, amendment, and complaints in consultation with the BSEE Associate Privacy Officer.

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 Information System Owner and Information System Security Officer are responsible for oversight and management of the security and privacy controls for this system. Authorized users are responsible for immediately reporting any suspected loss, compromise, unauthorized access or disclosure of data from the system in accordance with the rules of behavior and DOI policy. The BSEE Incident Response Manager coordinates the investigation of reported violations from users. The Incident Response Manager is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the BSEE Computer Security Incident Response Team and DOI-CIRC within one hour of discovery in accordance with federal policy and DOI procedures.