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: Everbridge Community Engagement Service (ECES)
Bureau/Office: Bureau of Indian Education (BIE)/Office of the Director
Date: December 23, 2022
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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 mission of the Bureau of Indian Education (BIE) is to provide students at BIE-funded schools with a culturally relevant, high-quality education that prepares students with the knowledge, skills, and behaviors needed to flourish in the opportunities of tomorrow, become healthy and successful individuals, and lead their communities and sovereign nations to a thriving future that preserves their unique cultural identities.

Everbridge Community Engagement System (ECES) is a voluntary cloud-based subscription application that uses text messaging to provide organizations with the ability to quickly send information to recipients, which may include students, parents or guardians, and faculty.

The BIE will use ECES to conduct and improve school community communication and engagement. A handout will be provided to parents and legal guardians of minor students,

faculty and administrators, and students that have reached the age of majority (18 years old). The handout describes the purpose of the service, includes a Privacy Act statement, and provides the Everbridge number and a keyword that the opt-in text is to be sent to become a Subscriber. Individuals become subscribers when they voluntarily text a keyword(s) to a provided subscription number (opting-in). At this time the number of the mobile device is recorded by ECES so the subscriber may receive future text messages. Once a subscriber completes the process to opt-in, they will receive automated text notifications of various school events and activities posted by the schools. Subscribers have the option to stop receiving subscribed to text messages by texting the word "STOP" to the previously provided subscription number (opting out). The subscriber does not have the ability to add any information to the subscriptions, so the subscriptions remain anonymous. Furthermore, School Administrators of the ECES cannot see the user's mobile number, only a count of how many users subscribed.

Everbridge is a FedRAMP authorized Software as a Service (SaaS) cloud service provider with all federal government data stored in the United States. The Department of the Interior (DOI) currently maintains the Authorization to Operate and PIA for Everbridge for DOI Employees and volunteers only. BIE is extending the use of this system to BIE-operated schools for notifications, such as school status, upcoming events, reminders, etc. This PIA is being completed for the BIE community engagement portion of Everbridge that is a separate virtual environment from the DOI Employee environment, and no information is shared between the two.

C. What is the legal authority?

Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications; the Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 USC 1401; OMB Circular A-130; 25 U.S.C. 1, 1a, 13; 25 U.S.C. 480; Public Law 95-561 and subsequent amendments; 25 CFR parts 31, 32, 36, and 39; the Snyder Act (25 U.S.C. 13); Johnson-O'Malley Supplemental Indian Education Program Modernization Act (25 U.S.C. 5301); Elementary and Secondary Education Act (20 U.S.C. 6301); Tribally Controlled Schools Act (25 U.S.C. 2501 et seq.); Indian Self-Determination and Education Assistance Act, as Amended (Pub. L. 93-638; Indian Education Amendments of 1978 (25 U.S.C. 2001 et seq.); Individuals with Disabilities Education Act (IDEA) (20 U.S.C. 1400 et seq.); Elementary and Secondary Education Act of 1965 (As amended through Pub. L. 115-224, Enacted July 31, 2018), and Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99).

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: Allow the use of Everbridge Community Engagement System Webtool to conduct and improve school community communications and engagement.

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

☒ No: The DOI Review Board approved Everbridge Visitor/Community Engagement as a Webtool.

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	Not Applicable	No	Not Applicable

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)*

ECES is not a Privacy Act system of record. However, some records pertaining to students, education staff, and parents or guardians used by ECES are maintained under DOI system of records notices INTERIOR/BIA-22, Native American Student Information System (NASIS), 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021) and DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), modification published 86 FR 50156 (September 7, 2021). These SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes: OMB Control Number 1076-0122, Data Elements for Student Enrollment in Bureau-funded Schools, Expires December 31, 2024.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number – Subscribers – Number Only, not tied to name or another unique identifier
☒ Other: Work Email Address – School Administrators.

BIE collects the minimum information necessary to manage the subscription service. Use of the service is voluntarily, and users can opt-out at any time. A handout will be provided to parents and legal guardians of minor students, faculty and administrators, and students that have reached the age of majority (18 years old). The handout describes the purpose of the service, includes a Privacy Act statement, and provides the Everbridge number and a keyword that the opt-in text is to be sent to become a Subscriber and begin receiving school notifications.

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:

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: (New Subscriber)

New Subscribers: The Personal Cell Telephone Number is collected automatically by the system when an individual chooses to opt into the service. A handout will be provided to parents and legal guardians of minor students, faculty and administrators, and students that have reached the age of majority (18 years old). The handout describes the purpose of the service, includes a Privacy Act statement, and provides the Everbridge number and a keyword that the opt-in text is to be sent to become a Subscriber and begin receiving school notifications. Individuals become subscribers when they voluntarily text a keyword(s) to a provided subscription number (opting in). At this time the number of the mobile device is recorded by ECES so the subscriber may receive future text messages. The phone number of the mobile device being used is automatically collected by the application. Numbers are collected anonymously; not tied to a name or other unique identifier. ECES School Administrators. The school will provide First Name, Last Name and business Email of the individuals chosen as School Administrators. This information may be provided by email or by telephone contact.

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

The mobile phone numbers are used in the transmission of Short Message Service (SMS) text messages to subscribers. The SMS text messages are about school-related information such as events, activities, reminders, etc., posted by school administrators. There is no PII in the content of the messages.

School Administrator First Name, Last Name and business email are collected to create a School Administrator account and to create and transmit text messages. There is no PII in the content of the messages.

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

☐ Within the Bureau/Office:

☐ Other Bureaus/Offices:

☐ Other Federal Agencies:

☐ Tribal, State or Local Agencies:

☐ Contractor:

☒ Other: ECES PII is not shared. ECES is a third-party application that stores subscriber mobile phone numbers in an encrypted database that is not accessible by BIE, other Bureaus, or Agencies. Collection is voluntary and is collected automatically by the system when an individual chooses to opt into the service.

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

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

The ECES is a voluntary self-subscription service. The only PII collected is the phone number of the mobile device used to subscribe. The service allows schools to send text messages relating to school events. Individuals can subscribe and unsubscribe at their discretion.

A handout will be provided to parents and legal guardians of minor students, faculty and administrators, and students that have reached the age of majority (18 years old). The handout describes the purpose of the service, includes a Privacy Act statement, and provides the Everbridge number and a keyword that the opt-in text is to be sent to become a Subscriber. Individuals become subscribers when they voluntarily text a keyword(s) to a provided subscription number (opting-in). Individuals can decline the Everbridge subscription number provided in the handbook thereby not completing the subscriber requirement to receive school notifications. Individuals become subscribers when they voluntarily text a keyword(s) to a provided subscription number (opting-in) and can opt-out anytime thereafter.

It also explains that the phone number of the device used to subscribe to the service will be retained until such time that the subscriber opts out. Students, parents, guardians, and faculty consent to voluntarily provide mobile device numbers to start the subscription service and receive the initial notification message from Everbridge to opt-in or opt-out. Consent is documented as part of the school admissions form.

School employees volunteering to be a System Administrator voluntarily provide their First Name, Last Name, and Work email address. A School Administrator Handout is provided that 1) explains the system and provide instruction on how to perform their function as a School Administrator; and 2) notify designated School Administrators that their First Name, Last Name, and business email will be collected to create a School Administrator Account. They will be able to have their PII removed from the system by notifying their Principal that they wish to be replaced as a School Administrator.

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

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 is included on the Data Elements for Student Enrollment in Bureau-funded Schools form (OMB Control Number 1076-0122, Expires 12/31/2024).

☒ Privacy Notice: A Privacy Notice will be included in the Subscriber and System Administrator handbooks to inform subscribers to review the Everbridge privacy policy to learn how Everbridge uses their information. Privacy notice is also provided through the publication of both this PIA and the publication of DOI-08, DOI Social Networks and BIA-22, Native American Student Information System (NASIS) SORNs.

☐ 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 the mobile phone number to allow the transmission of SMS text messages to subscribers. Subscribers and School Administrators do not have access to the mobile phone numbers.

Subscribers will have access to the SMS text messages published by the School Administrators. Subscribers will voluntarily opt-in to receive text notifications of school published information concerning school operations and activities. Subscribers may opt-out of the notifications at any time by texting the keyword STOP to the subscription phone number.

I. Will reports be produced on individuals?

☒ Yes: BIE will run reports on subscribers 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 numbers for deletion. The BIE 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?

Individuals voluntarily provide their mobile phone numbers when subscribing to the service. BIE presumes the information provided by individuals is accurate. The mobile number is retained in an encrypted database. It is not accessible by subscribers or school administrators. The mobile number is retained in the database until a subscriber opts-out; after which the number is removed from the database.

B. How will data be checked for completeness?

Information is obtained directly from individuals who voluntarily provide their mobile phone number when subscribing to the service. BIE presumes the information provided by the individuals is complete. The mobile number is retained in an encrypted database. It is not accessible by subscribers or school administrators. The mobile number is retained in the database until a subscriber opts-out; after which the number is removed from the database.

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

Information is obtained directly from individuals who voluntarily provide their mobile phone number when subscribing to the service. BIE presumes the information provided by the individuals is current. The mobile number is retained in an encrypted database. It is not accessible by subscribers or school administrators. The mobile number is retained in the database until a subscriber opts-out; after which the number is removed from the database.

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 ECES are maintained under 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.

The mobile number is retained in the encrypted database for the duration of the subscription. When a subscriber opts-out the number is automatically removed from the database.

The text messages are transitory in nature and are retained on the mobile device until deleted by the subscriber. The messaging system maintains a record of the text messages for 18 months. The messages are automatically deleted from the system after the 18-month period.

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

When a subscriber opts-out the number is automatically removed from the database. Text messages received by a subscriber are deleted from the mobile device at the discretion of the subscriber. Text messages, at the system level, are automatically deleted after 18 months. Approved disposition methods include electronic records with the Departmental Records Schedule 1, Departmental policy, and 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.

Everbridge has a "Low" system security categorization. This categorization is based on the limited, non-sensitive information collected and the requirement for security and privacy controls to protect the confidentiality, integrity, and availability of the 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 of 2014 (FISMA).

The ECES poses a low risk to the privacy of subscribers because of the limited PII used with ECES which is limited to the subscriber's mobile phone number. ECES subscribers voluntarily provide their mobile phone number to receive school notifications. The information is used to transmit one way SMS text messages involving school operation, events, and activities which contain no PII. There is also limited risk, with minimal impact, to the privacy of School Administrators who provide their Name and work email address. These risks are mitigated by a combination of administrative, physical, and technical controls.

There may be a risk associated with using a cloud service provider to manage the ECES. Everbridge is a Software as a Service (SaaS) cloud service provider located in the United States. Everbridge is FedRAMP certified. Everbridge has undergone a formal Assessment and Authorization in accordance with the FISMA and NIST standards. ECES is rated as a FISMA Low system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII. Everbridge has a current System Security and Privacy Plan documenting required security and privacy controls to protect the confidentiality, integrity, and availability of the PII maintained in the system.

There is a risk that individuals may not have notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published BIA-22, Native American Student Information System (NASIS) system of records notice, 73 FR 40605 (July 15, 2008), modification published 86 FR 50156 (September 7, 2021) and DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), modification published 86 FR 50156 (September 7, 2021), which may be viewed at: https://www.doi.gov/privacy/doi-notices. A Privacy Act statement is provided on the form (OMB Control Number 1076-0122) and on the Subscriber and School Administrator handbooks where consent is provided, and mobile numbers are collected from students, parents, guardians, and faculty. The PAS, PIA, SORNs, and Privacy Notice provide detailed descriptions of data elements and how an individual's PII is used.

In addition to the risk mitigation actions described above, the Bureau maintains an audit trail of activity sufficient to reconstruct security relevant events. The BIE follows the 'least privilege' security principle, such that only the least amount of access is given to a user to complete their required activity. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

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 data is both relevant and necessary to the purpose for which the system was designed. The service supports improved communications to the BIE schools by providing timely information regarding school operations, events, and activities.

☐ No

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

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

☒ 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?

Not Applicable. No new data is created.

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: Subscribers and School Administrators

Contractors, Developers and System Administrators will be provided access to the application and underlying database based upon their job function and the principle of least privilege.

Subscribers do not have access to the application or underlying databases. Subscribers receive text messages composed by School Administrators.

School Administrators have access to the application but not access to the underlying databases. The school administrators use the application to craft and transmit school messages.

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

Subscribers do not have access to the databases containing the anonymous mobile phone numbers and text history. Subscribers have access to the text messages crafted and transmitted by School Administrators. A handout will be provided to parents and legal guardians of minor students, faculty and administrators, and students that have reached the age of majority (18 years old). The handout describes the purpose of the service, includes a Privacy Act statement, and provides the Everbridge number and a keyword that the opt-in text is to be sent to become a Subscriber. Individuals become subscribers when they voluntarily text a keyword(s) to a provided subscription number (opting-in). At this time the number of the mobile device is recorded by ECES so the subscriber may receive future text messages.

The School Administrators will have access to the application to craft and transmit messages. They will be assigned this responsibility by school leadership. School Administrators do not have access to the databases containing the anonymous mobile phone numbers and text history.

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. ECES is a third-party application that is maintained by the owner. 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)
- 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. This service only sends messages to anonymous registered mobile numbers. The system has audit features that allow BIE 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 messages.

☐ No

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

Only 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 timestamp) 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. Access to text messages is limited to those individuals that subscribe to the service.

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.

(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.

(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.

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 BIE Deputy Associate Chief Information Officer is the Information System Owner. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for ensuring safeguards are implemented to protect individual privacy in compliance with Federal laws and policies. The ISO and the Privacy Act System Managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the IA 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 ECES ISO and ISSO are responsible for the central oversight and management of the ECES security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ECES ISO, ISSO, and bureau and office system administrators are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within one hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with IA Associate Privacy Officer. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act, the Family Educational Rights and Privacy Act (FERPA) and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.