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: ShakeAlert
Bureau/Office: U.S. Geological Survey/Earthquake Science Center
Date: September 28, 2018
Point of Contact:
Name: Stephen Guiwits
Title: Security Engineer
Email: sguiwits@usgs.gov
Phone: (626) 226-8023
Address: 525 South Wilson Avenue, Pasadena, CA 91106

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 U.S. Geological Survey (USGS), along with a coalition of State and university partners, is developing and testing an earthquake early warning (EEW) system called ShakeAlert. The purpose of ShakeAlert is to identify and characterize an earthquake a few seconds after it begins,

calculate the likely intensity of ground shaking that will result, and deliver warnings to people and infrastructure in harm's way.

Currently, the USGS and its partners are testing ShakeAlert on the West Coast of the United States, which has the highest risk of earthquakes in the country. An ecosystem of State and local governments and private entities, referred collectively as "organizations," are developing mechanisms that will alert people of earthquakes through mobile applications, browser-based tools, audio sirens, texts, and other automated system controls. Included with these alerts may be instructions to stop tasks, drop to the floor, take cover, hold on, or move away from hazardous objects or areas. In addition, alerts can be sent to automated systems that contain preset, situation-specific logic actuators developed and branded by third parties. The messages communicated in these alerts will usually be to slow or stop train, road, or air traffic, close valves, stop pumps, reduce spills, park delicate machinery in safe mode, or halt elevators.

ShakeAlert has been sending live alerts to "beta" users in California since January 2012 and in the Pacific Northwest since February 2015. The West Coast-wide "production prototype" has been designed for redundant, reliable operations. Product availability will expand on a region-by-region basis as soon as the ShakeAlert system, its products, and its parametric data meet minimum quality and reliability standards for the geographic regions in which ShakeAlert is to be deployed.

From a developer standpoint, ShakeAlert communicates with organizations that run on the Active Messaging Queuing Message Broker (AMQMB) software. The AMQMB works on a publish-subscribe model in which relevant notifications and alerts called "topics" are published for any number of users. When a specific email address initiates a "pull" from the AMQMB, it establishes an open socket to begin a continuous flow, or "push," of topics to a subscribing organization's AMQMB or client application, thus causing the subscribing organization to receive an Extensible Markup Language (XML) message.

To facilitate ShakeAlert's messaging protocol, the USGS and its collaborators utilize a function called ShakeAlert UserDisplay to display topics to users. The UserDisplay is a Java-based application that has been developed to receive XML-formatted messages and rapidly and simply display earthquake alert information that can be viewed on a user's computer.

The UserDisplay, as illustrated in Figure 1, shows the user's location and the estimated epicenter of the earthquake. As time elapses from the detection and notification of the earthquake, its compressional waves (small jolts called "P" waves) and shear waves (larger jolts called "S" waves) are also shown, as well as the expected magnitude of the earthquake, the estimated intensity of shaking at the user's site, and the remaining time until the shaking is expected to start.

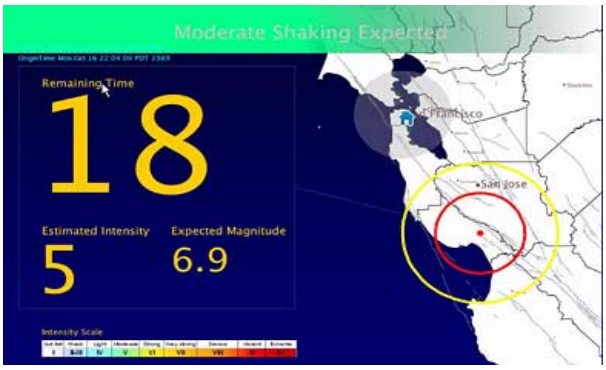

Figure 1: The ShakeAlert UserDisplay shows the user's location (house symbol), earthquake epicenter (red dot), P waves (yellow circle), S waves (red circle), estimated magnitude (6.9), estimated intensity (5), and remaining time until the shaking is expected to start (18 seconds) (Source: https://wwww.shakealert.org/).

The information described in this Privacy Impact Assessment (PIA) refers to the information that is currently collected from organizations using UserDisplay for proof-of-concept/pilot/test purposes. The same type of information will be collected for all organizations and their users going forward into the production phase.

C. What is the legal authority?

The United States Geological Survey (USGS) is tasked with developing an earthquake early warning system in the United States, as codified in the Earthquake Hazards Reduction Act of 1977, 42 U.S.C. §§ 7701 et seq. See: 45 U.S.C. 7701.

The most recent National Earthquake Hazards Reduction Program authorization (P.L. 108-360), a) notes the loss-reduction value of early-warning systems (sec 7701); b) specifically calls for disseminating warnings of earthquakes (sec 7702), and c) authorizes the USGS to establish and operate the Advanced National Seismic System "in order to enhance earthquake research and warning capabilities" (sec 7707) and for the authority to develop an EEW system.

The System of Records Notice used is Computer Registration System – Interior, GS-18, which is authorized by 40 U.S.C. 486(c) and 41 CFR part 201-7.

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

Unique Item Identifier Code: 010-000000987
System Security Plan: System Security Plan (SSP) for ShakeAlert

☐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	N/A	N/A	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)*

Computer Registration System – Interior, GS-18

☐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
☐Citizenship
☐Gender
☐Birth Date
☐Group Affiliation
☐Marital Status
☐Biometrics
☐Other Names Used
☐Truncated SSN
☐Legal Status

☐Place of Birth
☐Religious Preference
☐Security Clearance
☐Spouse Information
☐Financial Information
☐Medical Information
☐Disability Information
☐Credit Card Number
☐Law Enforcement
☐Education Information
☐Emergency Contact
☐Driver's License
☐Race/Ethnicity
☐Social Security Number (SSN)
☐Personal Cell Telephone Number
☐Tribal or Other ID Number
☐Personal Email Address
☐Mother's Maiden Name
☐Home Telephone Number
☐Child or Dependent Information
☐Employment Information
☐Military Status/Service
☐Mailing/Home Address
☒Other: *Specify the PII collected.* Organization Email Address, Internet Protocol (IP) Address

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
☒Other: *Describe* USGS Application, ActiveMQ Logging

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

The intended use of the personally identifiable information (PII) collected is to enable the user's organization to subscribe to ShakeAlert topics.

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

☒Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The ShakeAlert Communications and Outreach Manager at the USGS maintains the entire set of PII collected from the organizations outside of the ShakeAlert system in consideration of the A&A process. The Communications and Outreach Manager at the USGS shares this information with collaborators across the West Coast.

☐Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☐Contractor: *Describe the contractor and how the data will be used.*

☒Other Third Party Sources: *Describe the third party source and how the data will be used.*

Information including organization's IT personnel's name and email address will be shared with outreach personnel for university collaborators who support USGS activities related to ShakeAlert. Their data, which is maintained by the collaborators, is not part of the system that is seeking Assessment and Authorization (A&A) approval.

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

☒Yes: All information is voluntary. Information is not sent to web browsers but does traverse the general Internet. Several processes and agreements including the (a) ShakeAlert Pilot application, (b) ShakeAlert End User License Agreement and Terms of Service, (c) Pilot Partner Acceptance Letter, and (d) End User Check-list Process are in place to alert users of any personal information that they may be asked to contribute.

☐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: *Describe each applicable format.*

The following Privacy Act Statement is provided to end users looking to be approved as Beta Users of the ShakeAlert system:

Authority: This information is solicited under the authority of 42 U.S.C. 7701, P.L. 108-360, 40 U.S.C. 486 (c), and 41 CFR part 201-7.

Purpose: By providing the requestor's email address, the requestor is submitting information to the United States Geological Survey (USGS) to be approved to be a Beta User of the ShakeAlert earthquake early warning system. Once approved, the ShakeAlert system will store the email address along with the code (password). This will allow the requestor's organization to access and receive earthquake early alert topics of interest from the ShakeAlert ActiveMQ broker.

Routine Uses: Only ShakeAlert USGS system administrators and the requestor's local point of contact will have access to the email address and code (password).

Additional information on authorized routine uses may be found in the published system of records notice, GS-18, Computer Registration System, at 63 FR 29910, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-1998-11-09/pdf/98-29910.pdf#page=1. A new routine use was added to the system of records notice on May 19, 2009, which may be viewed at https://www.gpo.gov/fdsys/pkg/FR-2009-05-19/pdf/E9-11613.pdf#page=1.

Disclosure: Furnishing the information on this form is voluntary; however, failure to provide all or part of the information will not provide the organization access to the ShakeAlert system to access and receive earthquake early alert topics of interest from the ShakeAlert ActiveMQ broker.

☒Privacy Notice: *Describe each applicable format.*

Privacy Notice is provided through publication of this PIA.

☐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.).

A code issued by USGS only goes to the IT personnel's email address. Data is retrieved by ShakeAlert through organization's IT personnel's email address and a code issued by USGS to the organization's IT personnel's name. This data is within the A&A boundary reviewing AMQMB log files. The organization's IT personnel enters the email address and the code into the organization's software which reads the alerts from the USGS Active MQ broker system. As the user's email resides on the USGS Active MQ broker system, when the organizations' software reads (the subscribed topic) as a "read-only" messages from the USGS Active MQ broker system, the USGS Active MQ broker system recognizes the email and accepts the subscription request and will start publishing data on the topic of interest to the software on the subscribers end.

The organization's IT personnel's email address is also stored and may be retrieved from spreadsheets maintained by university collaborators and USGS outreach personnel, but this data is not within the scope of the system seeking A&A approval.

I. Will reports be produced on individuals?

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

The reports will be used to determine: (a) who is logging into the system, (b) how frequently a user logs in, and (c) to which server a user logs in. These reports help the USGS determine if accounts are no longer needed and show how well our load balancers are working.

☐No

Section 3. Attributes of System Data

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

There is no verification within the system that is seeking A&A approval as it is presumed that the user is submitting accurate data. Outreach personnel for university collaborators verify the data while they work with the organizations to ensure the organizations receive the alerts and are able to set up their applications to inform automation systems and users.

B. How will data be checked for completeness?

There is no check for completeness within the system that is seeking A&A approval as it is presumed that the user is submitting complete data. Outreach personnel for university collaborators verify the data while they work with their organizations to ensure the organizations receive the alerts and are able to set up their applications to inform automation systems and users.

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

The USGS expects the users in the interested organizations to update their information when changes occur.

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

User accounts are deleted when the USGS's or collaborators' outreach personnel request users be removed from the system. This retention period is consistent with the USGS General Records Disposition Schedule, Item 202-06b - User Identification, Profiles, Authorizations, and Password Files, Excluding Records Relating to Electronic Signatures. The disposition of these records is temporary, and the records are destroyed when the Bureau determines they are no longer needed for administrative, legal, audit, or other operational purposes.

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

All data is electronic and is deleted from the systems in which they reside. Data continues to remain in source code repository archives.

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.

The security and maintenance of this system is provided by a designated group of U.S. government administrators and they, along with the U.S. government information system owner, will protect and ensure the security of the privacy rights for this system. The overall impact to privacy is low. IP address and name could determine the location of a particular user. This information is fundamental to the system as it helps the USGS determine if the organization received an alert to be able to alert their users and systems within a certain zone. If the information is not shared, then the risk to the organization is that it will not receive an electronic email with the correct information needed to "subscribe" to the ShakeAlert server alert. When someone leaves an organization, the USGS usually gets a request to terminate that email and set up a new email for whoever fills the vacancy. The ShakeAlert system administrators also monitor the logs to check if the subscriber/software is authenticating into the ShakeAlert system using too many login attempts. If the USGS notices a large number of login attempts, the issue will be investigated. ShakeAlert system administrators monitor if the logs attempt access to the system that may amount to more than subscription (e.g., attempt to log in for write access). If the IP addresses do not appear valid or activity is suspicious, for the security of the ShakeAlert system, the subscribing organization 'communications and outreach coordinator' is contacted.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒Yes: *Explanation* Users are required to use the email address and token, i.e., software log-in information, to receive 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?

No new data; not applicable.

F. Are the data or the processes being consolidated?

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

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

☒No, data or processes are not being consolidated.

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

☐Users
☐Contractors
☐Developers
☒System Administrator
☒Other: *Describe* USGS University Collaborators if they ask

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

Users do not have access to their data.

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. The USGS collaborates with its collaborators, who are primarily universities. The development of the code occurs within the University of California Berkeley, the University of Washington, and the California Institute of Technology. The USGS has cooperative agreements with these collaborators.

☐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 AMQMB logs contain when the user logged in and their IP addresses. IP address and name could determine the location of a particular user. From this information, it could be possible determine where they are at a point in time geographically. This information is fundamental to the system as it helps USGS determine if the organization received an alert to be able to alert their users and systems within a certain zone.

☐No

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

The IT person's email address is collected. The system can then monitor the IP address from which the organization reaches the ShakeAlert system to subscribe to the alert. The organization shares when the IT person is no longer with them so that the subscription can be swtiched over to another email address or removed (if they no longer want to be a pilot project).

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

To prevent unauthorized monitoring, ShakeAlert systems are behind firewalls and have restricted privilege. Security measures and access controls consist of: passwords, user identification, whitelisted IP addresses, and software controls. All employees, including contractors, must meet the Privacy Act clauses for protecting Privacy Act-protected information.

The ShakeAlert system offers many security features, including but not limited to:

- Packet filtering via firewall and access lists on routers
- Intrusion Detection/Protection System accomplished with Suricata, an open system developed by the Open Information Security Foundation
- Network Access Control via OpenBSD Packet Filter servers and the IOS Cisco Control List
- Patching and configuration management of all computers that continue to be performed by government IT security personnel
- Root login that is limited to government personnel. The system restricts pseudo access to the local system administrator for emergency purposes and is controlled by the Puppet open-source software.
- Quarterly vulnerability scanning. Collaborator systems receiving and processing the earthquake waveform signals internally use the OpenVAS scanning tool for vulnerability management of devices.
- DOI/USGS oversight and their ability to validate patch and configuration status. The ShakeAlert government systems will be periodically scanned per U.S. government security standards. The USGS uses Nessus to conduct its vulnerability scans.
- All unneeded services on the system are turned off.
- All ports with outside access are blocked unless absolutely required by the AMQ Broker.

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* Secure server facilities

(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 ShakeAlert System Owner serves as the Information System Owner and the official responsible for oversight and management of ShakeAlert's security and privacy controls,

including the protection of information processed and stored by ShakeAlert. The Information System Owner and the ShakeAlert Privacy Act System Manager 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 ShakeAlert. The System Manager is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, 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 the USGS 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 ShakeAlert Information System Owner is responsible for oversight and management of the ShakeAlert security and privacy controls and for ensuring, to the greatest possible extent, that ShakeAlert 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 PII is reported to the USGS Computer Security Incident Response Team, preferably by the assigned Security Point of Contact, immediately upon discovery in accordance with Federal policy and established procedures.