ADAMS ML19338E212

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Everbridge Notification System (ENS)

Date: December 13, 2019

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Everbridge Notification System (ENS) allows the Nuclear Regulatory Commission (NRC) to notify employees and contractors of important events such as office or building closures, weather related event information, or any other emergency event that necessitates an emergency notification. In addition to the notification features, the system is also used to monitor personnel accountability during critical events and emergencies. ENS can provide geolocation through a mobile application for individuals that might be at risk and allows individuals to confirm their safety or availability during emergency situations by replying to the system notifications.

Registration in the notification system is mandatory for NRC employees while contractor participation is voluntary but highly encouraged. Employees and contractors register by entering their personal contact information into the NRC Enterprise Identity Hub (EIH) which transfers that data to ENS. Once individuals are registered as contacts, they will be able to receive short message service (SMS) text messages, emails, or voice messages from ENS. The ENS administrators can utilize various groups within the system to direct messages to appropriate contacts.

ENS is provided to NRC as a Software-as-a-Service cloud solution by Everbridge, Inc. The Everbridge cloud platform is authorized by the Federal Risk and Authorization Management Program (FedRAMP).

2. What agency function does it support?

ENS provides a clear and effective communication channel between the agency and its personnel during emergencies and other work-impacting events.

3. Describe any modules or subsystems, where relevant, and their functions.

ENS does not contain any modules or functions beyond its primary use for emergency communications.

4. What legal authority authorizes the purchase or development of this system?

Presidential Policy Directive 40 (PPD-40), National Continuity Policy, dated July 15, 2016 and U.S. Department of Homeland Security Federal Emergency Management Agency Federal Continuity Directive 1 (FCD-1) issued on January 17, 2017 require federal agencies to maintain a comprehensive and effective continuity capability including continuity communications.

5. What is the purpose of the system and the data to be collected?

ENS allows the NRC to communicate with employees and contractors during emergencies, abnormal situations, weather conditions, and/or dangerous events occurring at an NRC facility.

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
James Peyton	OCIO/ITSDOD/EPSB	301-287-0701
Technical Project Manager	**Office/Division/Branch**	**Telephone**
James Peyton	OCIO/ITSDOD/EPSB	301-287-0701
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Thomas Ashley	OCIO/ITSDOD	301-415-0771

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ____ New System

__X__ Modify Existing System

____ Other

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

A previous PIA was developed for the Verizon Notification Service (VNS). ENS will be replacing the VNS.

(1) If yes, provide the date approved and ADAMS accession number.

Approved March 27, 2012 (ML12067A167)

(2) If yes, provide a summary of modifications or other changes to the existing system.

The existing system that provides the critical event notification services (VNS) will be migrated to the Everbridge cloud platform.

8. Do you have an NRC system Enterprise Architecture (EA)/Inventory number?

No, ENS is an external Service

a. If yes, please provide Enterprise Architecture (EA)/Inventory number.

N/A

b. If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory number.

N/A

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Federal Employees and Federal Contractors.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

The following information about individuals is maintained in the system:

- Name
- Personal e-mail address
- Personal phone number(s)
- NRC e-mail address
- NRC phone number
- NRC office location, program office, NRC division, NRC LAN ID
- Time zone Information

c. Is information being collected from the subject individual?

Yes, individuals can modify and update their personal contact information in the EIH portal. The information is uploaded into ENS via an exported data file from EIH.

(1) If yes, what information is being collected?

The system collects individual contact information.

d. Will the information be collected from 10 or more individuals who are not Federal employees?

Yes, participation is mandatory for NRC employees. Contractors voluntarily enter their contact information.

(1) If yes, does the information collection have OMB approval?

OMB clearance is not required for subscription to an agency notification system.

(a) If yes, indicate the OMB approval number: N/A

e. Is the information being collected from existing NRC files, databases, or systems?

Yes

(1) If yes, identify the files/databases/systems and the information being collected.

Contact information will be collected from the NRC EIH.

f. Is the information being collected from external sources (any source outside of the NRC)?

No

(1) If yes, identify the source and what type of information is being collected?

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Individuals are expected to provide accurate contact information in order to be notified of critical events. Contacts have the ability to modify and update any inaccurate data from the EIH portal.

h. How will the information be collected (e.g. form, data transfer)?

Contact information will be collected by using the EIH data forms that can be accessed through the NRC Service catalog, and then it will be uploaded to ENS via a secure file transfer. Uploads will occur daily to ensure the latest information is made available in ENS.

EIH is a service under the NRC Identity Credential and Access Management (ICAM) System. For additional information regarding the system privacy data, refer to the ICAM PIA (ML19029A117).

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

Yes

(1) If yes, identify the type of information (be specific).

In addition to contact information, ENS will contain message templates and user groups.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

The ENS user groups and message templates are developed by organizational administrators.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

The data collected by the system will be used to notify NRC employees and contractors of important events such as office or building closures, weather related event information, or any other emergency that necessitates an emergency notification. Employees will be asked to respond to notifications with their status and/or availability to work in order to ensure accountability during an emergency situation.

Administrators can also provide contact information to individuals or groups outside of the NRC that are involved with accountability efforts such as local law enforcement.

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

Yes, data is used to provide situational awareness and directions to NRC employees and contractors through the critical notifications. Employees respond to notifications with their status and/or availability to work. Contact information can also be provided to individuals involved with accountability efforts such as local law enforcement.

3. Who will ensure the proper use of the data in this system?

Organizational administrators ensure that only authorized individuals are able to view user contact information and send notifications. Privileged users also account for the dissemination of contact information to other individuals with a "need to know".

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

Documentation will be made available on the Service Catalog page.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No. ENS does not aggregate data or create new data.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific)

Individuals can receive notifications from their group associations which can include geographical location, work or office location, and the individual's division or branch. Administrators can also retrieve individual contact information by name and other personal identifiers stored in the system

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes

a. If "Yes," provide name of SORN and location in the Federal Register.

Existing SORN, NRC 36, Employee Locator Records

8. If the information system is being modified, will the SORN(s) require amendment or revision?

SORN must be modified to include minor system location information

9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

Yes, ENS uses geolocation to identify the geographic location of individuals. Everbridge provides a mobile application that can be used to locate employees during an emergency and confirm their proximity to an event from their mobile device

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

This feature is only used by a limited number of authorized NRC staff to identify staff that might be at risk and is not enabled by default for all system contacts.

10. List the report(s) that will be produced from this system.

ENS administrators can produce various reports regarding the following:

- Successful and failed communications
- Logs pertaining to user actions (i.e. notifications, modification of templates, changes to system accounts)
- Responses to status and availability notifications
- Contact information

a. What are the reports used for?

Reports are used to ensure the system is functioning properly, and to manage and review access to the system, monitor staff accountability during emergencies and their availability to work. Reports are also used to disseminate necessary information to any individuals with a "need to know".

b. Who has access to these reports?

Only organizational administrators will have access to reports within the system. They will also manage permissions for other users that might have access to view specific reports. Reports can also be made available to entities outside the NRC that are involved in accountability efforts such as local law enforcement.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

A limited number of users within the Office of the Chief Information Officer (OCIO), the Office of Administration (ADM), the Office of the Chief Human Capital Officer (OCHCO), the Office of Nuclear Security and Incident Response (NSIR), and the regional offices will have access to ENS.

(1) For what purpose?

Staff will use ENS to create and manage groups based on location, office,

or other criteria in order to send out approved notifications to NRC personnel and manage communications.

(2) Will access be limited?

NRC employees and contractors that receive notifications will not have direct access to all data in the system. Only a limited number of users within the regional offices and NRC divisions will have the ability to send and receive communications or view user contact information.

2. Will other NRC systems share data with or have access to the data in the system?

Yes.

(1) If yes, identify the system(s).

ENS receives contact information from the EIH, a service which is managed under the ICAM system.

(2) How will the data be transmitted or disclosed?

Data is transferred through a secure FTP connection which encrypts the contact data during transmission.

3. Will external agencies/organizations/public have access to the data in the system?

Yes. The Cloud Service Provider, Everbridge, Inc., will have access to the data within the NRC tenant environment.

(1) If yes, who?

Everbridge staff.

(2) Will access be limited?

Everbridge ensures that its staff does not publicly publish customer data without approval by the NRC and ensures the the proper qualifications are met for staff that manage the NRC tenant.

(3) What data will be accessible and for what purpose/use?

As the Cloud Service Provider, Everbridge will have responsibilities related to the management and maintenance of the system. Everbridge can also send communications on behalf of authorized NRC staff during emergencies where access is unavailable. This allows Everbridge to

access agency personnel contact information.

(4) How will the data be transmitted or disclosed?

NRC does not transmit or disclose data in the system or permit Everbridge to share any agency specific data.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?

Yes

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).**

GRS 5.3 item 020 – Employee emergency contact information

Records used to account for and maintain communications with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers and addresses. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency situation.

Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee.

- For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?

b. **If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov**.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

ENS relies on the NRC ICAM system to provide single sign-on services for all on-premise NRC users. Users can access the system remotely through the ICAM Authentication Gateway using two-factor authentication through the use of a password and PIV, or one-time password credentials.

ENS will utilize a limited amount of cloud-only accounts in the event that ICAM cannot be accessed. These accounts will be accessible with a unique user ID and password and will be used only during an emergency when the primary method of authentication is unavailable.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

A limited number of global administrators have complete access to all data and privileges in the system. Global administrators will limit the number of users permitted to access the system contact information and send notifications. In addition, the system logs user and administrator access and actions in order to ensure accountability.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

The documentation regarding access to ENS will be completed during system migration to the Everbridge cloud platform. NRC personnel can access information related to the system on the agency service catalog.

The Cloud Service Provider has documented policies regarding the requirements for accessing the system. The documentation for the Everbridge Suite cloud product has been provided within the FedRAMP secure repository.

4. Will the system be accessed or operated at more than one location (site)?

The system is managed remotely by the Cloud Service Provider. NRC employees can access the system on-site at NRC HQ, Regional offices, and off-site through agency provided remote access technologies.

a. If yes, how will consistent use be maintained at all sites?

OCIO ensures consistent use of the system by preventing misuse of the system based on the granted permissions. Sub-administrators will have limited ability to make change or modify the system.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

The Contacts stored in the system will receive notifications, send replies, and have the ability to view their own contact information. System administrators will have the ability to modify user roles and privileges, manage users, and make minor modifications to the NRC tenant across all offices and groups.

Sub-administrators, assigned by the global system administrators, send notifications and manage information specific to groups to which they are assigned.

6. Will a record of their access to the system be captured?

Yes

a. If yes, what will be collected?

ENS logs all login activity, account lockout activity, password reset activity, and changes to account roles and privileges.

7. Will contractors be involved with the design, development, or maintenance of the system?

ENS is a cloud service developed and operated by a FedRAMP authorized cloud service provider. Contractors are involved in the design and development of the system.

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.

PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

A limited number of administrators within OCIO have access to all data and the management of agency-level privileges in ENS. Administrators manage the permissions for sub-administrators within the system. ENS uniquely identifies and authenticates users with access to the system.

Everbridge identifies and logs relevant user actions within the NRC instance. That information can be made available to agency administrators as needed.

9. Is the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

Yes, the Everbridge cloud service received an ATO from FedRAMP and a sponsoring federal agency on June 6, 2018.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: Everbridge Notification System (ENS)

Submitting Office: Office of the Chief Information Officer (OCIO)

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
This system contains Personally Identifiable Information and is retrieved by a personal identifier. ENS is covered by System of Records Notice, NRC 36, Employee Locator Records.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	2/13/2020

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

___ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	1/6/2020

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	1/15/2020

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

____ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date February 13, 2020

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Thomas Ashley, Director, IT Services Development & Operations Division, Office of the Chief Information Officer (OCIO)**	
Name of System: **Everbridge Notification System (ENS)**	
Date ISB received PIA for review: **December 18, 2019**	Date ISB completed PIA review: **February 13, 2020**
Noted Issues: The location information will need to be updated during the next review cycle for our system of records notice, NRC 36, Employee Locator Records. Since this is a minor change it does not require any immediate updates. OGC has been consulted and is in agreement with the determination.	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ February 13, 2020**
Copies of this PIA will be provided to: *Thomas Ashley, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Service Division* *Office of the Chief Information Officer*	