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.

Please do not enter the PIA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team.

Mass Notification System (MNS)

Date: April 28, 2022.

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system: (*Use plain language, no technical terms.*)

The Mass Notification System (MNS) is a Software-as-a-Service solution by Everbridge, Inc., used by the U.S. 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. MNS 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 MNS. Once individuals are registered as contacts, they will be able to receive short message service (SMS) text messages, emails, or voice messages from MNS. The MNS administrators can utilize various groups within the system to direct messages to appropriate contacts.

2. What agency function does it support? (*How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)*)

MNS 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.

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

a. Provide Agencywide Documents Access and Management System (ADAMS) ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.

N/A.

4. What legal authority authorizes the purchase or development of this system? (*What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.*)

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?

MNS allows NRC to communicate with employees and contractors during emergencies, abnormal situations, weather conditions, and/or dangerous events occurring at an NRC facility. The data to be collected from the employees and contractors will be personal identity information including name, home phone number, personal phone number, personal e-mail address, and personal SMS / text messaging service number.

6. Points of Contact: (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.*)

Project Manager	**Office/Division/Branch**	**Telephone**
James Peyton	OCIO/ITSDOD/NSOB	301-287-0701
Business Project Manager	**Office/Division/Branch**	**Telephone**
N/A	N/A	N/A
Technical Project Manager	**Office/Division/Branch**	**Telephone**
James Peyton	OCIO/ITSDOD/NSOB	301-287-0701

Executive Sponsor	Office/Division/Branch	Telephone
Thomas Ashley	OCIO/ITSDOD	301-415-0771
ISSO	**Office/Division/Branch**	**Telephone**
Natalya Bobryakova	OCIO/GEMSD/CSB/IAT	301-287-0671
System Owner/User	**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

____ Modify Existing System

__X__ Other

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

Yes.

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

A PIA was approved on May 12, 2021. The ADAMS accession number is ML21113A179.

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

The PIA has been transferred into the latest template and updated to include the most recent MNS authority to operate (ATO) information. Also, update to POC list.

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

Yes.

a. If yes, please provide the EA/Inventory number.

MNS is a subsystem of the Third-Party System (TPS). The TPS EA number is 20180002.

b. If, no, please contact EA Service Desk to get the EA/Inventory number.

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 [provide description for general public; non-licensee workers, applicants before they are licenses etc.]).

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 (<u>be specific</u> – e.g. Social Security Number (SSN), Place of Birth, Name, Address)?

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? (*To the greatest extent possible, collect information about an individual directly from the individual.*)

Yes.

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

The system collects personal contact information from the EIH portal, where individuals can modify and update their personal information.

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

Yes.

(1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?

OMB approval is not required. The current collection of information from contractors falls under the exemption to the Paperwork Reduction Act in 5 CFR 1320.3(h)(1). Collecting additional information from contractors on themselves or their emergency contacts may change this determination.

(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.

Personal contact information is collected from the NRC EIH where information is exported into a data file for uploading into MNS.

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

N/A.

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

N/A.

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 to be notified of critical events. NRC staff and contractors can modify and update any inaccurate data in the EIH portal.

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

Personal contact information is collected by using the EIH data forms which can be accessed through the NRC Service Catalog. The

information is uploaded to MNS via a secure file transfer. Uploads occur daily to ensure the latest information is made available in MNS.

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, MNS contains notification 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 MNS user groups and message templates are developed and modified internally by the organizational administrators and incident managers.

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 is 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 may be asked to respond to notifications with their status and/or availability to work in order to ensure accountability during an emergency. Administrators can provide contact information to authorized internal individuals for purposes of communicating regarding emergencies outside of the MNS application. This information will not be used for any "normal" communication, such as managers contacting employees regarding work assignments.

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 NRC emergency responders and local law enforcement.

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

The agency's MNS account administrators ensure that only authorized individuals can view user contact information and send notifications.

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 and information for MNS is made available on the NRC Service Catalog page. https://drupal.nrc.gov/ocio/catalog/25189.

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

No. MNS 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?

N/A.

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

N/A.

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

N/A.

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

Administrators will retrieve individual contact information by name and other

personal identifiers stored in the system to notify and locate contacts if necessary. Individuals will receive notifications from their group associations,based on location or other attributes.

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Individual names, geographical locations, offices, divisions, or branches will be used to retrieve information.

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.

a. If yes, explain.

MNS 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.

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

The feature is only used by a limited number of authorized NRC staff to identify individuals that might be at risk. Also, the feature is not enabled by default for all system contacts.

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

MNS administrators can produce various reports regarding the following:

- Successful and failed communications.
- Logs pertaining to user actions (i.e., notifications, modifications 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?

The system administrators have access to reports within the system. They also manage permissions for other users, such as incident managers, that might need access to view specific reports. Reports can also be made available to entities both inside and outside the NRC that are involved in accountability efforts such as NRC emergency responders and 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, the Office of Nuclear Security and Incident Response, and the regional offices have access to MNS. Data from MNS may be shared with other offices, as necessary, to facilitate responses to emergency situations.

(1) For what purpose?

Authorized staff use MNS to create and manage groups based on location, office, or other criteria, to send out approved notifications to NRC personnel and manage communication.

(2) Will access be limited?

NRC employees and contractors that receive notifications do 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. These

users can provide contact information to authorized internal individuals (e.g., NRC emergency responders) for purposes of communicating regarding emergencies outside of the MNS application. This information will not be provided as a normal course of business to NRC managers or others for use in non-emergency situations.

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).

MNS receives contact information from EIH, which 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) How will the data be transmitted or disclosed?

Data is transmitted through a Secure File Transfer Protocol connection which encrypts data during transmission.

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

Yes.

(1) If yes, who?

The cloud service provider (CSP), Everbridge Inc. has access to the data within the NRC tenant environment.

(2) Will access be limited?

Everbridge ensures that its staff does not publicly publish customer data without approval by the NRC and ensures 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 CSP, Everbridge has responsibilities related to the management and maintenance of the system. The Everbridge personnel can also send communications on behalf of authorized NRC staff during emergencies where access is unavailable. This allows the Everbridge personnel 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 United States Code (U.S.C.), 36 Code of Federation Regulations (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 and NARA's Universal Electronic Records Management 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 (GRS)?

Yes.

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

- **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?**

GRS 5.3 - Continuity and Emergency Planning Records

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.

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

b. If no, please contact the 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).

MNS relies on the NRC ICAM system to provide single sign-on services for all on-premises NRC users. Users can access the system remotely through the ICAM Authentication Gateway using two-factor authentication using a password and Personal Identity Verification (PIV) credentials, or one-time password credentials.
MNS will utilize a limited number of cloud-only accounts if 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?

MNS will utilizes role-based access control (RBAC) to authorize access to MNS based on a valid access authorization, intended system usage, and other attributes. A limited number of system administrators have complete access to all data and privileges in the system. System 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 to ensure accountability.

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

Yes.

(1) If yes, where?

NRC personnel can view information about the system on the agency service catalog.

The CSP has documented policies regarding the requirements for accessing the system. The documentation for the Everbridge Suite cloud product has been provided within the Federal Risk and Authorization Management Program (FedRAMP) secure repository.

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

No. The system is hosted and operated remotely by the CSP at one location.

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

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

MNS uses RBAC to issue user rights and privileges. The NRC Account Owner has established the role and membership requirements for each of the following account type on the platform:

- System account administrators have the ability to modify user roles and privileges, manage users, and make modifications and limited configurations to the NRC tenant across all offices and groups.
- Organizational administrators, assigned by the system account administrators, send notifications, and manage information specific to groups to which they are assigned.
- Incident managers, also assigned by the system account administrators, can view reports involving event notifications, users, and groups, modify templates, and create and assign tasks.
- The contacts stored in the system will receive notifications, send replies, and canview their own contact information through the EIH portal. Contacts do not have access to the system's data.

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

Yes.

a. If yes, what will be collected?

MNS 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?

MNS 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 Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (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 the administrators within OCIO have access to all data and the management of agency-level privileges in MNS. MNS uniquely identifies and authenticates users with the access to the system.

The CSP, Everbridge, identifies logs relevant to user actions with the NRC instance. That information can be made available to agency administrators as needed.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?

Yes, the Everbridge cloud service received an agency-sponsored authorization from FedRAMP on July 26, 2018.

NRC issued an ongoing authorization on December 30, 2021 (ML21364A164).

b. If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?

N/A.

c. If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.

N/A.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMSD/CSB Staff)

System Name: Mass Notification System (MNS).

Submitting Office: 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. MNS is covered by System of Records Notice, NRC 36, Employee Locator Records.

Reviewer's Name	Title
Signed by Hardy, Sally on 06/08/22	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:

As mentioned in prior PIAs, no clearance is currently needed for this system but that will likely change if ANY additional information is collected from Federal Contractors.

Reviewer's Name	Title
Signed by Cullison, David on 06/03/22	Agency Clearance Officer

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
Signed by Dove, Marna on 05/24/22	Sr. Program Analyst, Electronic Records Manager

D. BRANCH CHIEF REVIEW AND CONCURRENCE

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

__X__ 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:

Signed by Partlow, Benjamin on 06/15/22

Acting Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: Thomas Ashley, OCIO	
Name of System: Mass Notification System (MNS).	
Date CSB received PIA for review: April 28, 2022	**Date CSB completed PIA review:** June 7, 2022
Noted Issues: The location information will need to be updated during the next review cycle for the 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.	
Acting Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Partlow, Benjamin on 06/15/22
Copies of this PIA will be provided to: *Thomas G. Ashley, Jr.* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Garo Nalabandian* *Acting Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	