United States Environmental Protection Agency

# PRIVACY IMPACT ASSESSMENT

*(Rev. 2/2020)*
*(All Previous Editions Obsolete)*

Please submit your responses to your Liaison Privacy Official.
***All entries must be Times New Roman, 12pt, and start on the next line.***
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

| | |
|---|---|
| **System Name: Mass Alert Notification System (MANS)** | **System Owner: James Cunningham** |
| **Preparer: James Cunningham** | **Office: OMS-ARM/OA** |
| **Date: 09/06/2022** | **Phone: (202) 564-7212** |
| **Reason for Submittal: New PIA__ Revised PIA__X__ Annual Review____ Rescindment ____** | |
| **This system is in the following life cycle stage(s):** | |
| Definition ☐ Development/Acquisition ☐ Implementation ☒ | |
| Operation & Maintenance ☒ Rescindment/Decommissioned ☐<br><br>**Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).**<br><br>**The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).** | |

## Provide a general description/overview and purpose of the system:

The EPA Everbridge (MANS) system is a Software-as-a-Service platform that is used for managing critical events. The Environmental Protection Agency uses the MANS platform for operational response to critical events to keep individuals safe and business running smoothly. During public safety threats such as active shooter situations, terrorist attacks, or severe weather conditions, as well as critical business events such as IT outages, cyber-attacks, or other incidents such as product recalls or supply-chain interruptions, customers rely on the MANS platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications

processes, and track progress on executing incident response plans. In recent times, Everbridge's Covid-19 Shield packages (built within MANS) have provided return to-work, vaccine distribution, and other solutions to help customers successfully manage the Covid-19 pandemic. Many Federal agencies utilize MANS as part of their employee communication strategy – for the agencies' contingency planning and business continuity, staff augmentation, and IT Alerting needs.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The statutory authority for the Everbridge (MANS) system can be found in 44 U.S.C. 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.

## 1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

The System Security Plan (SSP) for the Everbridge (MANS) system has been developed and can be located in XACTA IA Manager Repository. There will be a new ATO for Everbridge upon completion of the FY22 SA.

## 1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required. ICRs are the responsibility and covered under the individual Programs.

## 1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, the data will be maintained and stored in the Everbridge Suite Cloud. The provider is FedRamp approved. The CSP will provide SaaS.

# Section 2.0 Characterization of the Information

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

## 2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

- First and Last Name
- Work Location (Building)
- EPA Desk Phone Number
- EPA Mobile Phone Number
- EPA Email Address
- Personal Mobile Phone Number (voluntary)
- Personal Home Phone Number (voluntary)
- Personal Email Address (voluntary)

## 2.2 What are the sources of the information and how is the information collected for the system?

EPA Phone Number Databases; EPA Email Database; EPA Active Directory; Individually Volunteered Information

## 2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources, such as information obtained from data aggregators. The system does not collect publicly available data, meaning information received from the internet, news feeds or from state or local public records, such as court records. Any data that resides in the Everbridge system have been collected from other EPA systems to determine the data's relevance to a particular matter, and the collected data may or may not include data that EPA has made or will make available to the public.

## 2.4 Discuss how accuracy of the data is ensured.

The data retained in the system are copies of information already residing on other EPA systems. Therefore, the accuracy of the data in the Everbridge system depends on the accuracy of the data in the source systems. Data is not modified in Everbridge as this tool is meant to be used by the Agency to provide emergency, non-emergency, and EPA Headquarters (HQ) accountability (per Federal Continuity Directive 1) process alerts and notifications, and mass alert and notification tests and drills, to Agency personnel at EPA HQ (EPA HQ personnel include EPA employees, contractors, and grantees).

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

*Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

**Privacy Risk:**

There is a risk that in the process to collect and determine whether information is relevant to a matter, more information is collected and maintained in the Everbridge Tool than is relevant to the matter.

**Mitigation:**

To mitigate this risk, the information that resides in the system that is determined not to be relevant to the matter will not be further disseminated beyond those individuals responsible for determining its relevance to the matter. Further, CIO Procedure 2155-P-03, Collection and Retention Procedures for Electronically Stored Information (ESI) Collected Using E-Discovery Tools, describes the data retention process for ESI collected using the Everbridge Tool. The information residing in the Everbridge Tool is necessary for providing emergency, non-emergency, and EPA Headquarters (HQ) accountability (per Federal Continuity Directive 1) process alerts and notifications, and mass alert and notification tests and drills, to Agency personnel at EPA HQ (EPA HQ personnel include EPA employees, contractors, and grantees). Part of the process includes determining relevance of the information and not all information will be determined relevant for the matter for which it was collected.

## Section 3.0 Access and Data Retention by the System

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

### 3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Access to the Everbridge system is restricted to a limited number of authorized users with the appropriate security clearances and password permissions. Access to the system is further limited by user type. System administrators have full access to the tool suite, including the ability to perform administrative functions. Other users have limited access particularized to the specific functions and data they need to perform in the tool. This access is controlled by a series of permissions within dedicated workspaces/databases for each specific request. Authorized users include federal and contract staff located throughout the country. The system is maintained in secure areas and buildings with physical access controls.

### 3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access controls the Cloud Service Provider, Everbridge Suite, has implemented for EPA Everbridge (MANS) are included in their SSP and approved as part of the Agency ATO and FedRAMP Authorization.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

There are no other components with assigned roles and responsibilities within the system.

### 3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Authorized authenticated Agency employees and contractors have access to Everbridge (MANS). Appropriate FAR clauses contained in the pertinent contracts govern use by contractors.

### 3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Users voluntarily participating in the system will maintain their own information and ensure it is accurate, relevant, timely, and complete. Bi-annual database management by system administrators will add new users and remove users no longer with the agency. Linking to the Active Directory will ensure accurate, relevant, and timely information is maintained within the system. No record control schedule number has been issued for the system.

### 3.6 Privacy Impact Analysis: Related to Retention

*Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.*

**Privacy Risk:**

Specific administration and support roles have access to user registration data.

**Mitigation:**

Rules of Behavior acknowledgement and Security Awareness training are required for key roles.

## Section 4.0 Information Sharing

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.*

### 4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No

### 4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

### 4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Disclosures of information residing in the Everbridge system are covered under EPA's General Routine Uses for records maintained in an EPA system of records and, therefore, memoranda of understanding or interagency agreements have not been issued for these purposes.

### 4.4 Does the agreement place limitations on re-dissemination?

There are no agreements in place and no information limitations apply for re-dissemination.

### 4.5 Privacy Impact Analysis: Related to Information Sharing

*Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?*

**Privacy Risk:**
None

**Mitigation:**
N/A

## Section 5.0 Auditing and Accountability

*The following questions are intended to describe technical and policy- based safeguards and security measures.*

### 5.1 How does the system ensure that the information is used as stated in Section 6.1?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behaviour, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

### 5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The US EPA implements a Rules of Behaviour (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness Training (ISPAT) which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

### 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

**Privacy Risk:**

Low risk of improper audit. There's a risk that the required information privacy controls may not be fully implemented or implemented properly.

**Mitigation:**

Privacy controls will be assessed prior to receiving an authority-to-operate (ATO) and as part of the NIST Risk Management Framework (RMF), continuous monitoring and annual security assessment will be conducted to ensure compliance with all privacy requirements.

## Section 6.0 Uses of the Information

*The following questions require a clear description of the system's use of information.*

### 6.1 Describe how and why the system uses the information.

The Mass Alert and Notification System is design to send voice and text messages to devices pre-selected by its users. The contact information data collected by the system will be used to ensure users receive EPA Headquarters emergency, non-emergency, and accountability information.

### 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes x No If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

EPA Email Address; the information is collected via system's secure web portal.

## 6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

MANS has an existing system of records notice, EPA-44. Everbridge has physical, technical, and administrative controls in place to protect privacy and to limit access. The MANS application is hosted in a FedRAMP cloud-based infrastructure hosted within AWS (Amazon Web Services) in the US. The physical security capabilities of AWS datacentre meet or exceed the EPA capabilities. Everbridge protects data in transit via TLS 1.2 using 256-bit Advanced Encryption Standard (AES-256). Administrative controls such as requiring role-based training, signing Rules of Behaviour (RoB) and restricting access to very small, limited number of approved Everbridge users and administrators.

## 6.4 Privacy Impact Analysis: Related to the Uses of Information

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

**Privacy Risk:**

None

**Mitigation:**

N/A

***If no SORN is required, STOP HERE.**

*The NPP will determine if a SORN is required. If so, additional sections will be required.*

# Section 7.0 Notice

*The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

## 7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

## 7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Federal and non-Federal individuals may opt out of sharing their information to register in the MANS.

## 7.3 Privacy Impact Analysis: Related to Notice

*Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.*

Individuals are given notice when they visit the online portal for purposes of registering in the information system.

**Privacy Risk:**

There is risk that individuals were not provided notice concerning the information they provide and its intended use.

**Mitigation:**

A link to the system of records notice is published on the web portal landing page giving individuals the opportunity to learn more about the uses of the information.

# Section 8.0 Redress

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

## 8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

## 8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

## 8.3 Privacy Impact Analysis: Related to Redress

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

No program exists for the project beyond the access and correction afforded under the Privacy Act and FOIA.

**Privacy Risk:**

N/A

**Mitigation:**

N/A