Privacy Impact Assessment

Emergency Alert System

May 23, 2023

Contact

D. Fon Muttamara
Chief Privacy Officer
Merit Systems Protection Board
1615 M Street, NW
Washington, DC 20419
privacy@mspb.gov

Abstract

The U.S. Merit Systems Protection Board (MSPB) is implementing a new emergency alert system utilizing the Everbridge Suite (Everbridge). Everbridge is a global provider of a Software as a Service platform for emergency communications. Such communications occur during events that affect MSPB's operations, man-made or natural disasters, and other emergencies affecting the workplace or employees. MSPB intends to leverage Everbridge to provide critical communications to MSPB employees when there is a need for mass notifications. These communications can be tailored to specific events and targeted to specific groups within the agency. MSPB is conducting this Privacy Impact Assessment (PIA) because Everbridge requires personally identifiable information (PII) from MSPB employees to send emergency alerts to them.

Overview

MSPB intends to use Everbridge to help manage emergencies using mass alerts and notifications. Everbridge will be managed by MSPB's Office of Financial and Administrative Management (FAM), which is responsible for, among other things, the security of personnel and physical locations. FAM will utilize Everbridge for operational response to critical events to ensure the safety and security of MSPB personnel and physical locations, as well as to keep MSPB personnel up to date on emergencies that may impact MSPB personnel and operations, such as active shooter situations, terrorist attacks, or severe weather conditions. FAM will determine, in conjunction with other affected MSPB offices, under what circumstances and when to send alerts. Individuals within FAM's management team will serve as the administrator of the system, have access to the data, and will draft alerts tailored to specific events or business needs. Additionally, each MSPB Regional Director and Chief Administrative Judge will have access to the data and have the ability to draft alerts tailored to specific events or business needs for their geographical location.

To utilize Everbridge, MSPB will collect the following employee contact information: MSPB-assigned office phone numbers, MSPB-issued mobile device numbers, MSPB email addresses, and MSPB duty locations. Employees may voluntarily provide their personal mobile number, home phone number, and personal email address. MSPB will not require employees to download or install mobile applications to their personal mobile devices, however, if individuals choose to voluntarily provide their personal mobile phone numbers, they have the option to download or install the Everbridge mobile application to their personal device. At this time, geolocation services will not be used to identify an individual's geographic location. Alerts will be sent in the following manner:

- MSPB email addresses: written alerts.
- MSPB-assigned office phones: recorded messages.
- MSPB-issued mobile devices: text alerts and recorded messages.
- MSPB-issued computers: pop-up written alerts.
- Personal email addresses, if provided: written alerts.
- Personal home phones, if provided: recorded messages.
- Personal mobile devices, if provided: text alerts and recorded messages.

To begin the initial PII collection, the Office of Information Resources Management (IRM) will provide a .csv file to FAM. The .csv file will contain MSPB employee email addresses and MSPB-assigned office phone numbers (and extensions if applicable) from MSPB's Microsoft Active Directory, as well as MSPB-issued mobile device numbers. FAM will then provide the file to Everbridge through MSPB's secure file sharing system, Box.com. As new hires onboard at MSPB, FAM will manually enter the required PII into the Everbridge system. Additionally, FAM will manually delete the PII of departing employees. Employees may voluntarily provide personal contact information, which FAM will add to the information maintained in Everbridge for those employees.

The privacy risks to the administration of this system have been mitigated through role-based access. Access to Everbridge is limited to the system administrators, i.e., specific individuals within FAM and IRM (the MSPB office responsible for providing technical support) who require access to the system in the performance of their duties. There is no anticipated sharing of the information stored in the Everbridge system outside of MSPB.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

MSPB's use of Everbridge is consistent with all applicable laws, regulations, and policies. The following legal authorities permit MSPB's use of Everbridge and define the collection of information in the system:

- 5 U.S.C. § 1204;
- Federal Continuity Directive (FCD) 1, Federal Executive Branch National Continuity Program and Requirements, January 17, 2017;
- FCD 2, Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process, June 13, 2017; and
- Directive on National Continuity Policy (National Security Presidential Directive 51/Homeland Security Presidential Directive 20), May 4, 2007.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

In accordance with the Privacy Act of 1974 (Privacy Act), MSPB proposes to establish a new MSPB SORN titled, "MSPB – 4, Emergency Alert System." This system of records contains information that MSPB collects, maintains, and uses for operational response to critical events to ensure the safety and security of MSPB personnel and physical locations, as well as to keep MSPB personnel up to date on emergencies that may impact MSPB personnel and operations, such as active shooter situations, terrorist attacks, or severe weather conditions. This system of records will be included in MSPB's inventory of record systems.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Everbridge has undergone Certification and Accreditation and was certified by the Federal Risk and Authorization Management Program Joint Authorization Board to operate at the Moderate impact level on June 7, 2018. IRM is responsible for maintaining the enterprise security Authorization to Operate (ATO) for this system and for implementing appropriate security controls. The ATO for Everbridge was approved by MSPB on March 9, 2022. A privacy risk assessment has been conducted on Everbridge through this PIA, which describes the measures that MSPB has taken to protect against privacy risks.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The information collected is subject to General Records Schedule 5.3: Continuity and Emergency Planning Records, Item 020 (Employee emergency contact information) – DAA-GRS-2016-0004-0002. These records are temporary and are destroyed when there is an update or upon separation or transfer of the employee.

1.5 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.

This is not an information collection under the PRA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The categories of individuals from which information is collected are MSPB employees. At this time, MSPB will collect the following contact information: MSPB-assigned office phone numbers, MSPB-issued mobile device numbers, MSPB email addresses, and MSPB duty locations. MSPB will not require personal contact information. However, if individuals volunteer to provide their personal contact information, that information will be collected, used, disseminated, and maintained by MSPB and Everbridge.

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

To begin the initial PII collection, IRM will provide a .csv file to FAM. The .csv file will contain MSPB employee email addresses and MSPB-assigned office phone numbers (and extensions if

applicable) from MSPB's Microsoft Active Directory, as well as MSPB-issued mobile device numbers. FAM will then provide the file to Everbridge through MSPB's secure file sharing system, Box.com. As new hires onboard at MSPB, FAM will manually enter the required PII into the system. Additionally, FAM will manually delete the PII of departing employees. Any collection of personal contact information will be voluntary. Employees may provide their personal contact information either during onboarding or any time during their tenure at MSPB.

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

No, the project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data is ensured by collecting the information from MSPB's Microsoft Active Directory, which is the agency's identity service provider. Additionally, the accuracy of data is also ensured by collecting personal information (personal phone number(s) and email) from individual employees during onboarding and at any time during an employee's tenure at MSPB.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This risk is partially mitigated. The information is collected from MSPB's Microsoft Active Directory and from the individual employee.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Employees' MSPB contact information will be used to send emergency alerts to employees for their safety and security. The alerts will be sent to employees' agency-assigned office phone numbers, cell phone numbers, and email addresses. Additionally, written alerts will be sent to agency-assigned computers via pop-up notifications. Emergency alerts also will be sent to employees' personal phone number(s) and email address if they have been voluntarily provided.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how MSPB plans to use such results.

The system will not use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or an anomaly.

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

No, there are no other MSPB components with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information will be used inappropriately.

Mitigation: This risk is partially mitigated. All system data is managed by FAM. The initial data entry of employee work contact information is overseen by Everbridge, but the information is provided by FAM in conjunction with IRM. Additionally, the system will have role-based access.

Privacy Risk: There is a risk that MSPB could use the information collected for purposes other than that for which the information was collected.

Mitigation: This risk is partially mitigated. MSPB will only utilize the information to the extent necessary to provide emergency alerts to MSPB employees. MSPB only collects PII that is directly related to the administration of the emergency alert system. All MSPB employees are required to take annual privacy training and are subject to discipline for inappropriately using PII. Additionally, access to the system and the PII in it will be limited to only the MSPB employees with a need-to-know to perform their official duties, specifically, to specific FAM employees, for the administration and use of the system, and specific IRM employees, to provide technical support.

Section 4.0 Notice

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

Individuals are provided written notice of the agency's collection of information through this PIA.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The information utilized by the system is information that has been generated and collected by MSPB to perform essential agency functions, such as an MSPB-assigned office and mobile telephone number and MSPB email address. Any personal contact information is provided

voluntarily, and the employee may consent to uses, decline to provide information, or have their personal contact information removed at any time.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that MSPB employees will not be given the opportunity to consent to the uses of their information.

Mitigation: This risk is partially mitigated. The information being collected is part of the employee's MSPB contact information, provided by MSPB for the employee to perform essential functions. Any personal contact information is provided voluntarily, and the employee may consent to uses, decline to provide information, or have their personal contact information removed at any time.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Upon separation from MSPB, employee information is removed from the system. The data is still maintained in Everbridge's Amazon Web Services environment until 30 days after the expiration of the contract. When MSPB's contract expires, MSPB's account will be deactivated and listed for deletion. Thirty days from the contract expiration date, MSPB's data will be flagged for purging and all the agency's data will be removed from the active system. Everbridge typically retains an organization's data for one month in the event the organization wishes to extend its subscription.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information collected by the system may be retained longer than is necessary.

Mitigation: This risk is partially mitigated. MSPB will manually remove any employee PII from the system upon separation from MSPB. Additionally, the information will be removed from the Everbridge servers after 30 days once the contract is completed.

Section 6.0 Information Sharing

6.1 Is information shared outside of MSPB as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No. PII is not shared outside of MSPB as part of normal agency operations. PII is only shared with external parties when required by a routine use in MSPB – 4, Emergency Alert System.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing noted in 6.1 denotes that information may be shared in a manner consistent with MSPB – 4, Emergency Alert System. External parties who receive access to PII collected under the SORN pursuant to a routine use are subject to the same Privacy Act limitations on disclosures as MSPB employees.

6.3 Does the project place limitations on re-dissemination?

Yes. MSPB places limitations on re-dissemination of PII. The information shared pursuant to the routine uses in MSPB's SORN is subject to limitations on further dissemination. MSPB outlines these limitations and obligations of the receiving party through a transmittal letter. Generally, receiving parties may not use the information for a reason not already approved by MSPB or further disseminate the information without the prior written consent of MSPB. Records released under a Freedom of Information Act (FOIA) request constitute public information, and MSPB has no authority to limit their re-dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

MSPB utilizes FOIAonline (https://foiaonline.gov/foiaonline/action/public/home) to track requests for information disclosure pursuant to the FOIA, the Privacy Act, routine uses in SORNs, or other applicable statutes and regulations. FOIAonline is a web-based application and assists MSPB in tracking and recording requests received for the disclosure of information. This includes requests subject to the accounting provisions of the Privacy Act. The information retained as part of this accounting requirement includes the agency or individual requesting the information, a description of the requested information, the reason for the request, the date of the request, the date of the release, the authority for the release, and the limitations and obligations on the requesting agency or individual with regard to use and further dissemination.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information will be shared outside the scope of the applicable SORN or without the proper authority or accounting.

Mitigation: This risk is partially mitigated. MSPB only shares information outside the agency as documented in this PIA and as permitted by MSPB – 4, Emergency Alert System. An accounting of disclosures is documented each time the information is shared outside the agency pursuant to the SORN in MSPB's FOIAonline system. Additionally, annual agency privacy training educates MSPB employees on the appropriate way to protect PII and information maintained in an agency system of records.

Privacy Risk: There is a risk associated with whether MSPB may be able to control Everbridge's retention of PII.

Mitigation: This risk is partially mitigated. MSPS's contract with Everbridge specifies that MSPB is the owner of all data collected and maintained. Everbridge is contractually required to destroy all information associated with any information collection 30 days after the end of the contract. MSPB also contracts for the right to investigate and audit a vendor's system to ensure they are complying with MSPB policies, procedures, and retention schedules. Any egregious or potentially illegal conduct could be referred to MSPB's Office of General Counsel or investigated by the MSPB Chief Privacy Officer (CPO).

Section 7.0 Redress

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

Individuals seeking notification of and access to their records in a system of records may submit a request in writing to the Office of the Clerk of the Board, Merit Systems Protection Board, 1615 M Street, NW, Washington, DC 20419. This request may also be sent to the agency by email at privacy@mspb.gov. Individuals requesting access must comply with MSPB's Privacy Act regulations regarding verification of identity and access to records (5 C.F.R. Part 1205).

Individuals will also be able to contact FAM, as the MSPB office responsible for human resources, to access the information FAM maintains on employees, including any personal phone numbers or email addresses provided by the individual.

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

Individuals seeking amendment of their records in a system of records may submit a request in writing to the Office of the Clerk of the Board, Merit Systems Protection Board, 1615 M Street, NW, Washington, DC 20419. This request may also be sent to the agency by email at privacy@mspb.gov. Individuals requesting amendment must follow MSPB's Privacy Act regulations regarding verification of identity (see Record Access Procedures above) and amendment to records (5 C.F.R. Part 1205).

Individuals will also be able to contact FAM, as the MSPB office responsible for human resources, to correct inaccurate information FAM maintains on employees, including any personal phone numbers or email addresses provided by the individual.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA provides notice to individuals on how to correct their information. Additionally, MSPB – 4, Emergency Alert System provides information to individuals regarding how to correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to correct inaccurate information that has been collected about them.

Mitigation: The risk is partially mitigated. Individuals may seek amendment of records that they assert are not accurate, relevant, timely, or complete by submitting an amendment request as outlined in MSPB's Privacy Act regulations at 5 C.F.R. Part 1205.

Privacy Risk: There is a risk that individuals will be unaware of the procedure for requesting access to the information that has been collected about them.

Mitigation: The risk is partially mitigated. This PIA provides information for individuals to understand how to seek redress, correction, or amendment. Additionally, MSPB's regulations and SORN providing the redress procedures are posted online.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

MSPB ensures that the practices stated in this PIA are followed by implementing training, standard operating procedures, policies, rules of behavior, and role-based access. Only employees and contractors with a valid need to know may collect and use information obtained from Everbridge. Moreover, any MSPB office or program that chooses to collect PII regardless of whether the activity requires PRA submission, is required to conduct a Privacy Threshold Analysis or a PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All MSPB employees and contractors are required to complete privacy awareness training when they onboard or begin working on an MSPB contract, respectively, and annually thereafter. MSPB's CPO logs all information governance training completed by agency personnel. This ensures that personnel are knowledgeable of their privacy, FOIA, and records management responsibilities, which includes their obligation to protect PII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

MSPB employees who have a need to know to perform their official duties will have access to the information maintained in Everbridge. MSPB deploys role-based access controls and enforces a separation of duties through all MSPB operations to limit access to only those individuals who have a need to know in order to perform their official duties. This need to know is determined by the respective responsibilities of the employee.

8.4 How does the project review and approve information sharing agreements, memoranda of understanding (MOUs), new uses of the information, new access to the system by organizations within MSPB and outside?

MSPB's use of Everbridge does not utilize information sharing agreements or MOUs. New uses of the information are not permissible without review and authorization by MSPB's Chief Information Officer and Senior Agency Official for Privacy. If new uses of the information are approved, they will only be utilized once appropriate notice has been provided, such as an update to this PIA or MSPB's SORN.

Responsible Officials

D. Fon Muttamara
Chief Privacy Officer
U.S. Merit Systems Protection Board

Approval Signature

WILLIAM SPENCER

Digitally signed by WILLIAM SPENCER
Date: 2023.05.23 13:36:49 -04'00'

William D. Spencer
Senior Agency Official for Privacy
U.S. Merit Systems Protection Board