Everbridge Mass Notification

*Privacy Impact Assessment*

August 29, 2019

POINT of CONTACT

Richard Speidel

*Chief Privacy Officer*
GSA IT
1800 F Street NW
Washington, DC 20405
Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application or project’s life cycle. The completed PIA demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA’s work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

Each section of the template begins with a statement of GSA’s commitment to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about [system, application or project name]. [GSA office] may, in the course of [program name], collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at: https://www.gsa.gov/portal/getMediaData?mediaId=167954

Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.
Table of contents

SECTION 1.0 PURPOSE OF COLLECTION
1.1 Why is GSA collecting the information? To maintain current information on

1.2 What legal authority and/or agreements allow GSA to collect the information?

1.3 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?

1.4 Has any information collection request (ICR) been submitted to or approved by OMB? If yes, provide the relevant names, OMB control numbers, and expiration dates.

1.5 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

SECTION 2.0 OPENNESS AND TRANSPARENCY
2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about them? If not, please explain.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

SECTION 3.0 DATA MINIMIZATION
3.1 Whose information is included in the system?

3.2 What PII will the system include?

3.3 Why is the collection and use of the PII necessary to the project or system?

3.4 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

3.6 Will the system monitor members of the public, GSA employees or contractors?

3.7 What kinds of report(s) can be produced on individuals?

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION
4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?
4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?
4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?
4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY
5.1 How will the information collected be verified for accuracy and completeness?
5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY
6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?
6.2 Has GSA completed a system security plan for the information system(s) supporting the project?
6.3 How will the system be secured from a physical, technological, and managerial perspective?
6.4 Are there mechanisms in place to identify security breaches? If so, what are they?
6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION
7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.
7.2 What procedures allow individuals to access their information?
7.3 Can individuals amend information about themselves in the system? If so, how?
7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING
8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.
8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING
9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?
9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?
Document purpose

This document contains important details about Everbridge Suite. The office of Mission Assurance (OMA) must collect and maintain personally identifiable information (“PII”) in order to assure its Continuity of Operations (COOP). PII is any information\(^1\) that can be used to distinguish or trace an individual’s identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA’s [privacy policy](#) and [program goals](#). The sections also align to the Fair Information Practice Principles (“FIPPs”), a set of eight precepts that are codified in the Privacy Act of 1974.\(^2\)

System, Application or Project

_Everbridge Mass Notification_

System, application or project includes information about

*GSA employees, Contractors, Summer Hires, Interns and Detailees*

System, application or project includes

_Names, personal telephone numbers (Opt-in), personal emails, and home addresses for contacting purposes_

SECTION 1.0 PURPOSE OF COLLECTION

_GSA states its purpose and legal authority before collecting PII._

1.1 Why is GSA collecting the information?

_OMA maintains up-to-date contact information on GSA employees and other persons covered by this system for use during a public or personal emergency. Only persons with national and local emergency management responsibilities may use the system to notify GSA officials, employees, and other affected individuals during such emergencies._

1.2 What legal authority and/or agreements allow GSA to collect the information?

Everbridge is covered by the following directives:


2) GSA ADM 2430.3 General Emergency Management Program

3) ADM 2430.1A: The U.S. General Services Administration Continuity Program

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Yes, those with national and local emergency management responsibilities can look a person up by their name and see their Zip Code and personal telephone number (if they opt-in). Group records are retrieved by organizational code (e.g. Federal Acquisition Service staff are labelled as “Q”). Everbridge is covered under GSA Credential & Identity Mgmt System (GCIMS) SORN GSA/CIO-1.

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No, as this is not an information collection under the Paperwork Reduction Act.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

Yes. Information maintained by the application is regularly updated with the last version of PII retained in the system for 30 days. (PII Extract Logs (GRS 04.2/140 - DAA-GRS-2013-0007-0013). The business need to retain that information ceases after 30 days (testing of upload of newer version materials, backup, etc.) and it and the original source data is purged from the Everbridge system and any related files.
Change logs (additions, deletions, updates, etc.) records related to that update of data are retained for 18 months for business purposes in accordance with Information Technology Development Project Records; System Development Records (GRS 03.1/011 - DAA-GRS-2013-0005-0007) and then purged from the Everbridge system.

Backups of both the entire master file and database are retained for 30 days in accordance with Backups of Master Files and Databases (GRS 3.2/051 - DAA-GRS-2013-0006-0008).

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

Yes. There is some risk in transmitting the CSV file containing emergency contact information from GCIMS to Everbridge, however, the privacy risks have been assessed and mitigated:

1. PII Abstracts from GCIMS are downloaded into a secure zip file, managed within an Excel Spreadsheet, and uploaded into Everbridge via a secure encrypted transmission using WINSCP. Both the zip file derived from GCIMS and the staging file from Excel are purged 30 days after uploading into Everbridge.
2. After uploading the source information into Everbridge, the previous version of the data is retained for 30 days and then purged. The operational and administrative tasks associated with this update are retained for 180 days and then purged.
3. Data backups for this application are maintained for 30 days and then purged by the vendor.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.
Yes. The entire notice states: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of information contained herein may be used as a basis for physical access determinations. GSA describes how your information will be maintained in the Privacy Act system of record notice published in the Federal Register at 73 FR 35690 on June 24, 2008. Disclosure of the information by you is voluntary. Failure to provide information requested on this form may result in the government’s inability to account for you in case of national or local emergencies.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Yes, potential risks stem from access to PII. However, this risk is adequately limited by using Role Based Access Control (RBAC). The contract administrator establishes the roles. Further measures to mitigate the risk, the system is monitored, audited, and protected according to GSA IT policies and NIST requirements for IT systems.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Federal employees, Contractors, and Summer Hires, Interns and Detailees.

3.2 What PII will the system, application or project include?

Names are collected in Everbridge and individuals opt-in to provide any emergency contact information that they would like to keep on file.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

GSA’s emergency notification system requires current contact information for GSA employees and other persons for use by persons with emergency management responsibilities. GSA maintains this information only to notify officials, employees, and other affected individuals of conditions that require their urgent attention during a national or local emergency.
3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No, the system will not aggregate new data about individuals.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

Only individuals who have a minimum background investigation (MBI) are granted permission to the system. Access Logs are available for audit. Failed login attempts are set to a maximum number and continued failed attempts to login will result in being locked out/denied access until the account access for that user is unlocked by a system administrator.

3.6 Will the system monitor the public, GSA employees or contractors?

No.

3.7 What kinds of report(s) can be produced on individuals?

Everbridge provides the capability to create reports based on all information provided for an individual’s record. These reports are only available to those who have been approved for access to the application. No one may create reports without first being approved for access to the application.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

No. Reports will include the names of individuals so that they can be contacted in an emergency situation.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

The purpose of the application is to first notify our GSA community of an emergency and then to account for them. Each notification has a selected subset of people to notify and account for which limits the amount of PII required. Given the reporting capability, the security and privacy measures include access controls, awareness and training for users and auditing capability to ensure accountability.
SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Everbridge limits information only to what is required to send out notifications.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

No, GSA uses this emergency contact information for internal purposes only. However, the GCIMS SORN does allow for permissive routine uses which do not require the individual’s consent: https://www.federalregister.gov/documents/2014/08/12/2014-19079/privacy-act-of-1974-notice-of-updated-systems-of-records

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

GCIMS is the primary authoritative source. Although, please note for Gov’t employees information updated in HR Links is transferred to GCIMS.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

No. The only interaction occurs when a comma separated file (CSV) is uploaded into the Everbridge System from GCIMS.

4.5 Are there any privacy risks for this system, application or project that relates to use limitation? If so, how will GSA mitigate these risks?

Yes, GSA outlines appropriate uses and access controls for PII whenever it enters into agreements with third parties; for example, through data-sharing agreements, MOAs, or contracts. GSA does verify that their shared systems operate under the same NIST standards that our own platforms must be certified and compliant.
GSA requires that Everbridge uses a suite of automated tools are used to scan the systems for the latest known security vulnerabilities and provide follow up for mitigation. Encryption is a critical piece of the security posture and is updated or upgraded as older protocols are sunset.

Whenever possible, software code is used to replace humans when processing data to minimize the leakage of PII. The goal is to refine and remove access to PII to the greatest extent possible while still balancing business efficiencies and customer responsiveness.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

The information that Everbridge uses is directly from GCIMS, it is manually uploaded from GSA to Everbridge via csv file using the WINSCP application database. Everbridge inherits the data quality and integrity steps that GCIMS PIA specifies and is included in the following:

The GSA HSPD-12 Handbook describes processes to update information in case of employment events for both employees and contractors which in-turn result in an update of personnel data. Also the Identity, Credential, and Access Management (ICAM) Division plans to periodically verify GSA personnel eligibility for GSA Access Card by validating with various Staff and Service Offices. Additionally, the HR system provides a nightly download of all departing employees which helps the data in GCIMS to keep up to date. GSA personnel can also update their “Self Service” information as needed or required. Records with missing information will be flagged as incomplete until missing information is provided. Contract Information Worksheet (CIW) has all required information that is required by GCIMS. Incorrect data can be compared to the CIW for completeness. Business rules are coded into the data fields to determine the accuracy and completeness of inputted data. Twice a year, Point Of Contacts must verify with the HSPD-12 Program Management Office that their personnel records are still up-to-date or provide updates.
5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

There are no additional privacy risks related to data quality and integrity. However, GCIMS does attempt to mitigate unforeseen issues by classifying users into different categories. These classifications support the technical control concepts of Separation of Duties, Least Privilege, and Accountability. Each category of user has a distinct set of roles and responsibilities that determine the information to which they have access and the actions they are permitted to perform.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

GSA’s Office of Mission Assurance (OMA) Emergency personnel, GSA Emergency coordinators (ECs) and alternates, Deputy Regional Directors (DRDs) and their alternates and Everbridge Technical Support Staff. The information stored in Everbridge is only used to make emergency calls, agency notifications, alerts or quarterly drills, exercises & tests. Audit trails regarding who has gained access are available for review by trusted employees.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, GSA has completed system security plan (SSP) for the systems that support and maintain the information used in Everbridge. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). Everbridge operates on systems rated “moderate impact.” Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” to secure its systems and data.
6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

GSA assesses information and systems for compliance risk, reputational risk, strategic risk, situational/circumstantial risk, and operational risk. In order to mitigate these risks to an acceptable level, GSA implements extensive security controls for information collected or maintained on its behalf, and conducts third-party assessments of vendors and services it procures.

GSA leverages FedRAMP instance of Everbridge and it has been approved to use as SaaS from FedRAMP, GSA implements controls relevant to third party vendors and services according to risks identified the following types of third party reviews: Third Party Security Assessment and Authorization (SA&A) Package; Statements on Standards for Attestation Engagements (SSAE) Review; Risk Assessments by Independent Organization; or a complete Risk Assessment by GSA.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

GSA has procedures in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any confirmed or suspected incidents or breaches of PII directly to ITServiceDesk@gsa.gov or 866-450-5250.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.
7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

Both Government employees and contractors have access to their PII data by logging into the GCIMS application. Human Resources and the Office of the CIO frequently remind people to change their PII information as it changes to include:

1. Home Address

2. Home Phone (Mobile) - Opt In

Certain business information is only changed by Human Resources for Government employees. For Contractors, GCIMS is modified by an approved Contract Officer of Record (COR) or a designated Government admin who has approval by the division head or executive.

Government employees and Contractors initially opt-in at their time of employment or entry into a contract with GSA. Anytime during their work with GSA they may enter GCIMS to delete the information only in the PII designated fields. When this happens the daily CSV file delivered to GSA will have all the business information for that individual, but will no longer have any PII information. The CSV file completely replaces all fields for the user during the upload and installation of the file. The previous data from the day before is completely replaced. When individuals are no longer with GSA, their GCIMS record is marked "inactive". Inactive records are no longer provided in the CSV file that will be imported into Everbridge.

7.2 What procedures allow individuals to access their information?

Individuals can take their own personal information out of GCIMS. Their business information cannot be erased.

7.3 Can individuals amend information about themselves? If so, how?

Individuals can take their own information out of GCIMS, since GCIMS is the source of the Everbridge data. All individuals who have been issued a GSA PIV card can access their records using the GCIMS website. The HSPD-12 help desk has a phone number that can be contacted to request information be corrected or updated on individuals.
7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Yes. Organization leaders, Project lead, System manager, Emergency Coordinators and Regional emergency coordinators have access to PII information and may share certain data with individuals who may have a need to know, but are not cleared to have access during a time where non-confirmed individuals are trying to be located. For example in a severe weather event where people are not responding, there may be a reason to attempt to locate persons using their personal cell (if provided) or personal email.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

GSA requires annual privacy and security training for all personnel and has policies in place that govern the proper handling of PII. This is managed through the CIO and Online Learning University system.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

Any Everbridge staff that has access to customer data must complete a series of training modules on privacy, including protecting Federal PII. Under the training category for Everbridge Privacy Training the following areas are covered:

1. Ethics

2. Privacy

3. General Data Protection Regulation (GDPR)

4. Federal Personally Identifiable Information (Federal PII)

5. Personally Identifiable Information (PII)

6. Health Insurance Portability and Accountability Act (HIPAA)
SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA’s Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes, persons performing accountability and auditing will have elevated privileges in the Everbridge system.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit Everbridge and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA’s Privacy Office. In addition, access to PII information is curtailed or aggregated as needed for the specific purpose of the audit being performed.

---

[1] OMB Memorandum Preparing for and Responding to a Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.” The memorandum notes that “because there are many different types of information that can be used to distinguish or trace an individual’s identity, the term PII is necessarily broad.”