Everbridge Mass Notification

Privacy Impact Assessment (PIA)

September 4 , 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business 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 shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

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. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.**

Stakeholders

Name of Information System Security Manager (ISSM):

- Nate Ciano
  nathaniel.ciano@gsa.gov

Name of Program Manager/System Owner:

- Arthur (Buddy) King
  arthur.king@gsa.gov

Signature Page

Signed:

DocuSigned by:
Nathaniel Ciano
113E72276281433...

Information System Security Manager (ISSM)

DocuSigned by:
Arthur R King Jr
43A6E8841293437...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

Table of contents

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

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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?

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about *Everbridge Suite*. The Office of Mission Assurance (OMA) must, in the course of *Emergency Communications*, collect personally identifiable information (PII) to assure its Continuity of Operations Plan (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, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

Everbridge Manage Bridge is listed in GEAR and is listed under the GSA brand name as the National Alert and Accountability System (NAAS). Everbridge is included within the FISMA System Enterprise Application System (EAS).

B. System, application, or project includes information about:

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

C. For the categories listed above, how many records are there for each?

Approximately 18,000 to 20,000 GSA personnel. Approximately 4K records are not used for the purpose of notification for this application. Non-embedded contractors are removed from the database records. These are contractors on a contract with GSA, but do not occupy a physical GSA leased or owned building. The following table shows the exact totals for August, 6, 2020.

GSA Personnel - 08/06/2020	
Employees	11813
Detailees	145
Contractors - Embedded	3568
Contractors - Non-Embedded	4173
Summer Hires	1
Interns	1
Totals	19701

D. System, application, or project includes these data elements:

First Name, Middle Initial, Last Name, all GSA business contact information and the following (Opt-in) personal information:

1. Personal home phone and cell numbers
2. Personal email
3. Personal home address.

The business and home contact information supports the ability to locate the physical location of people during an emergency situation. For example, Everbridge allows GSA staff with national and local emergency management responsibilities to draw a circle on a map and alert staff in office space within that circle and those who have opted to provide their home addresses. .

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

- 5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 40 U.S.C. 3101, 40 U.S.C. 11315, 44
- U.S.C. 3602, E.O. 9397, as amended, and Homeland Security Presidential
- Directive 12 (HSPD–12).
- Everbridge is covered by the following directives:
- Federal Continuity Directive 1 (FCD-1) Annex K, Testing
- GSA ADM 2430.3 General Emergency Management Program
- ADM 2430.1A The U.S. General Services Administration Continuity Program
- ADM 2430.2 The U.S. General Services Administration Continuity of Operations Mission Essential Functions

1.2 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?

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 the member opts-in). Group records are retrieved by organizational codes such as Major Group (e.g. Federal Acquisition Service staff are labelled as “Q”) and Office Symbols such as IDTIC. Everbridge is covered under GSA Credential & Identity Mgmt System (GCIMS) SORN GSA/CIO-1.

1.3 Has an 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.

1.4 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 needs to retain that information ceases after 30 days (testing of upload of newer version materials, backup, etc.) 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 5 years 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 after imaged by a newer master file and database in accordance with Backups of Master Files and Databases (DAA-GRS-2013-0006-0008, GRS 3.2/051).

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes. GCIMS contains the notice of 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.

SECTION 3.0 DATA MINIMIZATION

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

OMA maintains up-to-date contact information on GSA employees and other persons covered by this system for use to notify officials, employees, and other affected individuals of conditions that require their urgent attention during a national or local emergency. Notification may be required during non-duty hours which means contacting people at their home location will be required.

3.2 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.

3.3 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.

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

No. The system will not monitor the public, GSA employees, or contractors.

3.5 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.

Everbridge is able to produce reports that can include PII. These reports are used to determine if people have received a notification and possibly how they respond to the notification. A time stamp provides the time and a confirmation value can be added to the report. The main purpose of reports is to find or contact people during an emergency who have **NOT** confirmed. GSA is required to fully report to personnel who need to be contacted. GSA personnel (OHRM) take action to contact people in actual emergencies using the **Not Confirmed** report.

It is possible to monitor the success or failure of active notifications. Depending on the time limit set by the sender, it is possible to stay on-line with a monitoring (30 second screen refresh) of the number of people who respond during this period. It is also possible during this period to create a report of the confirmations or non-confirmations during the period the notification runs.

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.

3.6 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.

SECTION 4.0 LIMITS ON USING AND SHARING 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?

Yes. 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)?

Government employee's information updated in HR Links is transferred to GCIMS. GCIMS is the single authoritative source.

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

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

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, maintained, used, or disseminated 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 Secure FTP application. 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.

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.

The Everbridge Contract Admin category has the authority to add people to the application. Their GSA Roles are: Contract Officer of Record (COR) and the Application Owner.

When Everbridge Government users terminate their employment or Contractors are terminated from a contract, they are automatically removed from access to the Everbridge application. Everbridge users must have the ability to log into GSA via 2-Factor Authorization (2FA) or via their Personal Identity Verification (PIV) card.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes. Everbridge has a System Security Plan (SSP). The EAS ATO was signed
March, 26, 2020 and expires on March 25, 2023.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

The information in the Everbridge database is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information.

Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security.

For example, The Everbridge platform uses Amazon Web Services (Amazon EC2) key pair to support our WINSCP Secure FTP transmission when exporting our input .CSV file into their designated cloud server. Amazon EC2 uses 2048-bit SSH-2 RSA Keys for the secure FTP transfer.

In addition, within GSA’s email platform PII information to external recipients can now be identified as having PII. If the email with PII in an attachment is not encrypted, a notification will appear to the user in the subject line stating PII Blocked Email Notification and the email will not be sent. The attachment must be FIPS 140-3 Compliant Zip file to securely send PII and Controlled Unclassified Information (CUI) to external recipients.

Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. GSA staff off-site may access GSA outside the firewall via a secure virtual private network (VPN) connection as well as by a CITRIX connection using GSA’s Virtual Desktop also known as VDI.

GSA staff regularly review GSA’s system audit records for indications of inappropriate or unusual activity.

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

GSA's Enterprise Information Operations (EIO) leverages the GSA Incident Response (IR) guide. In case of a suspected security incident/breach of PII, the IT Service Desk as well the Privacy Office and Incident Response team are notified immediately to start investigations.

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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, 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:

- Home Address
- Home Phone (Landline and 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?

Government Employees may delete their PII information from HR Links. Contractors may also delete their PII information from GCIMS.

HR Links information is transferred daily to GCIMS which is the sole source of information for the Everbridge application. Government and Contractor information exists in a single location to support the Everbridge application.

Business information cannot be deleted by the user.

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.

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.

In addition, GSA IT’s Rules of Behavior is included in the required security training and policies in place that govern the proper handling of PII.

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 owner ensure that the information is used only according to 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.

[1] OMB Memorandum *Preparing for and Responding to the 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.”

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.