Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. 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]

[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.

General Information

PIA Identifier: 343
System Name: National Alert and Accountability System (NAAS)
CPO Approval Date: 10/7/2022
PIA Expiration Date: 10/6/2025

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Erika Dinnie

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
National Alert and Accountability System (NAAS)

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.

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:

- Personal home phone and cell numbers
- Personal email
- 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.

Overview:

The Everbridge Suite (EBS) system is a set of software applications that have the purpose to automate and accelerate a Federal Agencies or organizations' operational response to critical events in order to keep people safe and businesses running faster. 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 EBS system functions 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.

1.0 Purpose of Collection

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?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
GSA Credential & Identity Mgmt System (GCIMS) SORN GSA/CIO-1.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.
As this is not an information collection under the Paperwork Reduction Act.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
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).

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.
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.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
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?
No

3.2 Explained: If so, how will this data be maintained and used?
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?
None

3.4 Explain: Please elaborate as needed.
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?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
ISSO Must complete on next recertification.

3.6 Why Not: Why will the data not be de-identified?
The data cannot be de-identified as Everbridge is used 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.

4.0 Limits on Using and Sharing 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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
This information wil not be shared

4.3: Is the information collected:
From Another Source

4.3Other Source: 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?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?

The only interaction occurs when a comma separated file (CSV) is uploaded into the Everbridge System that originated from GCIMS.

5.0 Data Quality and Integrity

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.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
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.

6.1b: What is the authorization process to gain access?
System administrators validate and approve access for users with business need to access Everbridge. This is a manual process via email and not an automated process via ServiceNow.

Administrator/master accounts are created by Everbridge after notification by the GSA account administrator.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/26/2020

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?
Yes

6.4What: 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.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
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.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that 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?
Yes

7.3How: How do individuals amend information about themselves?
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

8.0 Awareness and Training

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.

9.0 Accountability and Auditing

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.