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: 466
System Name: US Notify
CPO Approval Date: 4/8/2024
PIA Expiration Date: 4/8/2027

Information System Security Manager (ISSM) Approval

Sergio Mendoza-Jimenez

System Owner/Program Manager Approval

Amy Ashida

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
US Notify

B: System, application, or project includes information about:
US Notify allows federal and state agencies to send notifications to members of the public.

For Public Users, the information contained in the system includes:

- The contact details needed for delivery of the notification, currently email address or phone number.
- The notification message that may include customer service, official information dissemination, and/or product outreach information

Data is cached within the US_Notify system while sending the message to the contact address, and is never stored in the system's database.

US_Notify does not support the sending of sensitive data, such as:

- Social Security Numbers (SSN),
- Driver's license or state identification number; Alien Registration Numbers;
- Financial account number or information
- Protected healthcare information

For Federal and State Agency Users the information contained in the system includes authentication information, including contact details as well as access IP address.

C: For the categories listed above, how many records are there for each?
US_Notify does not store any contact details in its database. This number and content of messages in the cache will vary based on notifications sent by each agency.

Agencies are responsible for keeping the authoritative long-term records related to notifications and content.

D: System, application, or project includes these data elements:
The following PII information is provided by agencies to send an individual a notification:

- Phone number or email address
- Any PII necessary to convey meaning in the notification, especially first name, or agency appointment dates and locations.

The following PII information is collected when a federal or state government agency employee registers for a US_Notify account:

- First and Last name
- .gov email address
- Telephone number
- IP address

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Federal Citizen Services Fund (40 U.S. Code § 323), E-Government Fund (44 U.S. Code § 3604).

US_Notify does not collect information from the public. Agencies who utilize US_Notify are responsible for such collections.

Projects under this subsection may include efforts to—

(A) make Federal Government information and services more readily available to members of the public (including individuals, businesses, grantees, and State and local governments);

(B) make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and (C)enable Federal agencies to take advantage of information technology.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
No

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

1.2b: Explain why a SORN is not required.
US_Notify is not a system of record for any of the data uploaded by customer agencies. Customer agencies are responsible for maintaining their own records. Members of the public do not have access to the system.

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.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Notification sent through US_Notify are never stored in the system's database. Responsibility for retaining records lays with the customer agency.

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? No

2.1 Explain: If not, please explain.
US_Notify does not collect information.

Customers agencies are responsible for giving notice to individuals about the collection, maintenance, use, or sharing of personal information, including the dissemination of any information via US_Notify.

3.0 Data Minimization

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

Use of US Notify requires contact information, phone number or email address in order to deliver notifications to those phone numbers and/or email addresses.

US_Notify itself does not collect information from the public.

Agency users may include additional non-sensitive PII in the content of messages sent via US Notify.

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?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
In accordance with the Federal Information Security Management Act of 2002 (FISMA), every GSA system must receive a signed Authority to Operate (ATO) from a designated GSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program.

Additionally, Protections to protect the data:

* DB and file storage are encrypted in transit and at rest.

* Content in the database is additionally encrypted at the field level and redacted from display in reports and administrative UI

* Message data is not stored in the database

* Protections for unauthorized access:

* Accounts must be created with .gov email addresses

* Accounts must have multi-factor authentication

* Accounts are defined with roles and responsibilities that limits their access to only that which they have a need-to-know within their own agency services.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
No, the system does not provide the capability to monitor an individual.

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

Reports can be run on notifications sent to a specific phone number or email address. These reports include the name of the template that was sent to them and when it was sent. Specific message contents are not included in the report. This data is only stored for a short duration in order for agency users to validate the delivery of messages.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
Detailed reports are deidentified by omitting message contents. Aggregate usage reports are deidentified by not including notification message contents or the delivery email/phone contact information.

3.6 Why Not: Why will the data not be de-identified?

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?
Federal Agencies

4.2How: If so, how will GSA share the information?
Federal and State agency users will be able to run reports on notification messages that they have sent through the system.

US Notify will only receive information from other federal and/or state agencies. These agencies can see their own data in the system, but not other agencies data.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
Federal and/or state agency users will provide the information.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?

Federal and State agencies will send us information through uploading CSV files containing lists of notifications to send, as well as direct API integration to send notifications.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

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

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
Customer federal and/or state agencies are responsible for for verification of accuracy and completeness before using that information to send notifications through US_Notify.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
* Agency users have access to data that they upload into the system, until it is purged following our data retention policies.

* US_Notify platform administrators can access reports of notifications sent by any given service. These reports do not include actual message contents.

6.1b: What is the authorization process to gain access?
* US Notify Platform Administrator accounts are limited to federal employees and contractors on the US Notify team. Granting a user this level of access needs to go through the standard code change management process.

* Customer agencies gain access through the agreements process, including a formal MOU, which grants them m access to a trial mode that does not allow sending notifications to the general public. The service can then request to go live, and a US Notify Platform Administrator can grant them access to sending notifications to members of the public.

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.
8/30/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
US_Notify's physical security is provided by its cloud service provider cloud.gov. US_Notify's cloud service provider is FedRAMP authorized and provides US_Notify with logically separate infrastructure to separate it from other systems.
US_Notify manages technological security via a defense-in-depth approach, minimizing access at every level, with strong encryption of data both in transit and at rest. By maintaining strict control over the flow of information at every

step within the system, US_Notify is able to provide robust technical security. Additionally, US_Notify undergoes regular continuous monitoring activities to identify vulnerabilities. The US_Notify team remediates identified vulnerabilities within GSA defined timeframes based on severity.
User account requests for Platform Administrators and the first agency user must be approved by the System Owner. User account requests for additional service users are the responsibility of the customer agency for proper approval and assigning the appropriate roles to those users. All user roles and permissions must be reviewed and certified annually. User access requires multi-factor authentication.

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?
US_Notify has an incident response plan and conducts incident and breach response exercises. The system utilizes built in tooling from its cloud service provider and from cloud based monitoring tools to identify potential incidents and breaches.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
The GSA Privacy Office develops privacy policies and manages the GSA privacy program. The GSA IT Security Policy and GSA requirements for PIAs, SORNs, Privacy Act Statements, Annual Reviews of system notices ensure that GSA identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice for which the individual has provided consent. If consent is not provided by the individual, then the collection of information will not take place.
Members of the general public can consent or decline to provide information to the customer agencies through those agency's policies. Customer agencies are responsible for gathering consent to send notifications to the recipients. Individuals can additionally opt-out of receiving notifications from a phone number through US_Notify by responding to a text message notification with the word 'STOP'. Opt-outs are handled and enforced at the carrier level.

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?
Individuals must request access to their information from the customer agencies.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

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.
The GSA Privacy Office develops privacy policies and manages the GSA privacy program. GSA has developed, implemented, and regularly updates, develops, implements, and updates IT Security Awareness and Privacy Training 201, a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities. All GSA account holders electronically sign the GSA Rules of Behavior before taking privacy training exit exams. GSA privacy training includes targeted role-based privacy training for personnel having responsibility for PII and ensures that personnel certify acceptance of responsibilities for privacy requirements.

GSA mandates all employees to complete annual Security and Privacy Awareness Training. It provides training on how to Share Data Securely in a Collaborative Environment.

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?

US_Notify regularly reviews its operations to ensure that they meet the requirements outlined in this PIA. Program leaders and developers are held accountable for adhering to privacy best practices related to data minimization, transparency, and timely, effective notice. For example, US_Notify has created a transparent system built upon an open-source platform so that interested parties can advise the program. US_Notify engages developers and other interested parties through a public source code repository, which includes a public forum for discussion of the project. US_Notify is designed to operate on user profile, permissions, and agency services. Access and permissions are based on agency affiliation as well as need-to-know to perform job duties within US_Notify. User access and related permissions are reviewed and certified annually.