Notify.gov

GSA

Technical Overview

Updated: 4.25.24

Notify.gov is a federally-managed web-based text messaging platform that allows federal, state, local, tribal, and territorial governments to send one-way SMS notifications.

Agencies that sign up will be able to create and use personalized message templates for sending notifications.

The platform is managed by the Public Benefits Studio, within the Technology Transformation Services Division of the General Services Administration.

This document provides a basic technical overview of the Notify.gov system. For additional privacy, security, or other technical documentation please contact the Public Benefits Studio.

Federal Security Review

Notify.gov operates under a Lightweight Authority to Operate (LATO). This federal security authorization process leverages security controls provided by National Institute of Standards and Technology (NIST). The process is focused on operational security from both a functional and assurance perspective.

System Data

To send a message, agencies upload a spreadsheet of phone numbers and other necessary data from their existing data management system. On Notify.gov, data is encrypted when it passes through the service and when it's stored on the service. Notify.gov is not a system of record and as a result does not have a SORN. Agencies are responsible for managing their data outside of Notify.gov.

Any recipient data uploaded is only held for seven days; all PII is deleted for successful messages, so data is retained only for unsuccessful messages.

- Notify stores data within the cloud.gov-managed PostgreSQL database and S3 buckets. The entire database is encrypted at the disk level.

- Additionally, data is encrypted at the field level when it is stored in the database, using OpenSSL 3.0.8 via the Python cryptography library. The implementation is available on GitHub.

Basic infrastructure

Notify.gov is comprised of two applications both running on cloud.gov:

- Admin, a Flask website running on the python_buildpack which hosts agency user-facing UI
- API, a Flask application running on the python_buildpack hosting the Notify API

Notify.gov utilizes several cloud.gov-provided services through Amazon Web Services (AWS):

- AWS S3 buckets for temporary file storage
- AWS Elasticache (Redis) for caching data and enqueueing background tasks
- AWS RDS (PostgreSQL) for system data storage

Notify.gov also provisions and uses two AWS services via a supplemental service broker:

- AWS SNS for sending SMS messages
- AWS SES for sending email messages (note: email function is currently unavailable to users for pilot)

Two-way messaging & replies

Under LATO, Notify.gov cannot receive incoming messages. This means that two-way messaging is not possible.

If a recipient does reply, AWS SNS is able to provide an autoresponse. This can be configured by Notify.gov staff. As an AWS internal configuration, this is not exposed in the Notify.gov UI.

Opting out of messages

Recipients may opt out of receiving text messages by responding with “STOP” to any message. AWS SNS manages opt outs, but some phone carriers additionally manage opt outs internally. If a message recipient is accidentally opted out, or wishes to restart messages, it’s necessary to check both places:

- Notify.gov staff opts in the phone number in the AWS dashboard
- The recipient sends a “START” text message to the sending phone number

Notify.gov does not yet have a way to pull opt-out status and make it available in the UI for agencies to download.

User permissions and signing-in

Notify.gov users access the platform by creating an account via web browser. You can set different user permissions in Notify including who can send messages, edit templates and add team members. This lets you control who in your team has access to certain parts of the service.

Notify.gov uses Login.gov to deploy enhanced security protections to protect your Notify.gov account. Login.gov is an extra layer of security created by the government that uses multi-factor authentication and stronger passwords to protect your account. Other government agencies, such as the Social Security Administration and the Small Business Administration, already use Login.gov to provide secure access to their government services.

Multi-factor Authentication

Multi-factor authentication (sometimes referred to as "two-factor authentication") adds an additional layer of security to your account by requiring another piece of information along with your username and password to log in. Using Login.gov, Notify.gov users can choose between one of the following:

- **Phone number:** Get a unique, one-time code by text message or phone call. If you are not using a mobile phone that can get text messages, please choose to get your security code by a phone call.
- **Authentication application:** Get temporary security codes from an app on your device (smart phone, computer, tablet, etc.).
- **Security key:** A security key is usually a piece of physical hardware, like a USB, that you can carry on your keychain. You can also use supporting software, such as a web browser extension or other services. The security key must be compatible with the FIDO standard.
- **Government employee ID:** If you are a government employee and used your government email address to create your account, you will have the option to use your government employee PIV/CAC card. Connect your card to your device using a card reader and enter your existing PIN.
- **Backup codes:** We will give you a list of 10 codes that you must keep in a safe location. Each time you sign in, we will ask you to enter one of the codes. After you use all 10, we will give you 10 new codes. Note: backup codes are the least secure option and are not recommended unless you don't have access to the other options.

Sensitive information

Some messages include sensitive information like security codes or password reset links.If you’re sending a message with sensitive information, you can choose to hide those details on the Notify dashboard once the message has been sent. This means that only the message recipient will be able to see that information.