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: 490
System Name: Permitting.gov
CPO Approval Date: 11/6/2024
PIA Expiration Date: 11/6/2027

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Gerard Chelak

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Permitting.gov

B: System, application, or project includes information about:
Permitting.gov includes information about GSA Employees, Contactors and Members of the public.

C: For the categories listed above, how many records are there for each?
11 Records: 1 Record for each Admin user

Permitting Council have three (3) forms that are publicly available and publicly accessible: The forms are intended for users to voluntarily communicate with the permitting council.

Contact Form: # is unknown at this time

FAST-41 Initiation Notice (FIN) Form: Approx. 100 or less yearly

Permitting Council Feedback Survey Form: # is unknown at this time

The number of records are subject to change. However, Permitting Council estimates that there will be approximately hundreds (100s) to Thousands (1000s) or records.

D: System, application, or project includes these data elements:
Name, Email Addresses (Personal and/or Business Email Addresses), Business, Physical Address (No Personal Address), Phone numbers (personal and/or Business) and DAP (Universal Government Agency Instance of Analytics), along side Permitting Council Google Analytics.

Overview:

Permitting.gov is a public facing Drupal website providing communication, public relations outreach and inbound marketing. It will service the Permitting Council's publishing needs to communicate permitting related information with other agencies and the public.
The application resides on the GSA ECAS II Core, which is housed within the FedRAMP, approved AWS US East infrastructure. AWS provides all physical security controls associated with protecting Permitting Council's application, as well as various other support services such as alternate processing sites, alternate storage sites, and computing environments. permitting.gov leverages the following AWS services for operations through the ECAS II environment: S3, IAM, EC2, VPC, EBS, RDS, Cloudformation, Autoscaling, KMS, and Elastic Load Balancer (ELB). All data is stored encrypted and only transmitted over encrypted methods. All data is stored in Amazon and as such the encryption of the stored data is handled by and is the responsibility of Enterprise Content Application System II (ECAS II) platform.
Access to the AWS management console is provided to ECAS II administrators in order to properly administer the associated AWS services. This administration can include monitoring, validating and configuring AWS. Access is granted to the console via AWS IAM service. In accessing the AWS console, an ECAS II administrator must enter his/her credentials followed by the required One Time Password (OTP) token. This permits access to the management console to perform required administration activities to the AWS services.
Permitting Council (administrators and developers) users who require access to the ECAS II require associated Sophos SSL VPN credentials. These credentials, when applied, provide the GSA users with access to core services such as Jenkins, and access to internal application URLs. IAM Access keys may be granted to allow access to application specific staging buckets to provide files to ECAS II administrators for project purposes.
Permitting Council collects Personally Identifiable Information (PII) via three (3) forms that are publicly available and publicly accessible: The forms are intended for users to voluntarily communicate with permitting council. Personally Identifying Information (PII) (i.e., email message containing a question or comment or completing a site form that emails us information) collected are used to respond to user's requests. Emails collected may be forwarded to other Federal Government (Permitting Council) employees who are better able to answer the user's question(s). Information collected from users are not given to any private organizations or private persons. Information are not collected or used for commercial marketing. Statistical information collected will be used to help provide an even better online experience for users.
Permitting Council Forms:

- **Contact Form:** https://test.permitting.gov/about/contact-us
- **FAST-41 Initiation Notice (FIN) Form:** https://test.permitting.gov/helping-you/apply-now/fin
- **Permitting Council Feedback Survey Form:** https://test.permitting.gov/permitting-council-feedback-survey

There is no System of Record Notice. However, there is a Privacy Policy link at the bottom of each of the forms. https://test.permitting.gov/privacy-policy.

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. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

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.

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.
Dispose of in accordance with the approved disposition instructions for the related subject individual's records, or 5 years after the disclosure for which the accountability was made, whichever is later.

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.
Information collected is provided voluntary. There is a Privacy Policy Link at the bottom of the site that displays the form.

https://test.permitting.gov/privacy-policy

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
Contact Form: The ability to reach back out to the user who submits the form. Information collected on the contact forms are not displayed publicly but rather available to authenticate Drupal Admin Console users.

FAST-41 Initiation Notice (FIN) Form: Carrying out permitting council's mission.

Permitting Council Feedback Survey Form: Used to provide better online experience

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?
Drupal generates unique identifier for all data within the system. The IDs are not publicly visible, they are not sensitive information and are only used within the system.

All data is stored encrypted and only transmitted over encrypted methods. All data is stored in Amazon and as such the encryption of the stored data is handled by and is the responsibility of ECAS II platform. All encryption keys are configured to be managed to GSA standards within AWS managed services.

Role-Based access only via Drupal login. An application warning banner has not been configured.

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

3.4 Explain: Please elaborate as needed.
There is no monitoring capability - The application cannot identify, locate or monitor individuals.

3.5 What kinds of report(s) can be produced on individuals?
There are no reports produced on individuals and as such there is no monitoring log - The application does not have any monitoring capability (e.g., cross-device tracking) to produce a report on an individuals.

The Information on the Contact Form is used to reach back out to the user who summited the form. Information collected on the contact forms are not displayed publicly but rather available to authenticated Drupal Admin Console users.

The information on the FAST-41 Initiation Notice (FIN) Form is used to carry out permitting council's mission.

The information on the Permitting Council Feedback Survey Form is used to provide better online experience.

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?
Drupal generates unique identifier for all data within the system. The IDs are not publicly visible, they are not sensitive information and are only used within the system.

All data is stored encrypted and only transmitted over encrypted methods. All data is stored in Amazon and as such the encryption of the stored data is handled by and is the responsibility of ECAS II platform. All encryption keys are configured to be managed to GSA standards within AWS managed services.

3.6 Why Not: Why will the data not be de-identified?
Information collected is voluntary. De-identified of data (name, email address, business address and/or phone number) are not obscured.

Data such as Name, Email Addresses (Personal and/or Business Email Addresses), Business, Physical Address (No Personal Address), Phone numbers (personal and/or Business) collected voluntarily are not de-identified (obscured)

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?
Information will only be shared with the Permitting Council employee(s) only.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

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?
Permitting.gov integrates with Flickr, a Service Site API call that connects to Flickr API and downloads certain contents and catches it within the Drupal system for presentation to public users (Photos for public users to view). In general, the integration provides support for browsing album content retrieved from the Flickr API.

Album and photo content are retrieved within page controllers from the Flickr service pc.flickr.api. The service provides two public methods for use within page controllers. The public methods in turn make use of a number of private methods that access the Flickr API directly.

API Usage:

Permitting.gov implementation results in API requests for the following actions in the following amounts.

- **Retrieving All Album Ids -** 1 Call per 500 albums available in the configured user account
- **Retrieving Subset of Album Details (For Paging) -** 1 Call per page (# of albums / # of albums per page)
- **Retrieving Individual Album Details -** 1 Call per album page
- **Retrieving Individual Album Photos -** 1 Call per album page

Flickr is a public image hosting service provided by a Third Party related to DOT. Permitting.gov have unique credentials they use to access it but services are available to the public as it's a commercial company.

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

4.4NoAgreement: Why is there not a formal agreement in place?
Based on CIO 2100.1P Policy dated January 31, 2024
A formal documented ISA is not required. Information exchange is web-based services via API. Connection is approved when the SSPP/ATO is approved.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
There is no automated mechanism in place. Verification is done manually

6.0 Security

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

6.1b: What is the authorization process to gain access?
Admins are provided authorization on a as needed basis. (Permissions and roles are assigned). Authorization will follow authentication.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
No

6.2a: Enter the actual or expected ATO date from the associated authorization package.

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Permitting.gov resides on the GSA ECAS II Core, which is housed within the FedRAMP, approved AWS US East infrastructure. AWS provides all physical security controls associated with protecting Permitting Council's application, as well as various other support services such as alternate processing sites, alternate storage sites, and computing

environments. permitting.gov leverages the following AWS services for operations through the ECAS II environment: S3, IAM, EC2, VPC, EBS, RDS, Cloudformation, Autoscaling, KMS, and Elastic Load Balancer (ELB).
All data is stored encrypted and only transmitted over encrypted methods. All data is stored in Amazon and as such the encryption of the stored data is handled by and is the responsibility of Enterprise Content Application System II (ECAS II) platform.
Access to the AWS management console is provided to ECAS II administrators in order to properly administer the associated AWS services. This administration can include monitoring, validating and configuring AWS. Access is granted to the console via AWS IAM service. In accessing the AWS console, an ECAS II administrator must enter his/her credentials followed by the required One Time Password (OTP) token. This permits access to the management console to perform required administration activities to the AWS services.
Permitting Council (administrators and developers) users who require access to the ECAS II require associated Sophos SSL VPN credentials. These credentials, when applied, provide the GSA users with access to core services such as Jenkins, and access to internal application URLs. IAM Access keys may be granted to allow access to application specific staging buckets to provide files to ECAS II administrators for project purposes.
Permitting.gov will implement the required security and privacy controls according to NIST SP 800-53. The systems employs a variety of security measures stated above and also defined in the System Security Privacy Plan (SSPP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, along with system and information integrity.

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?
The system owner and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer, along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Information is provided "At will"
A Privacy Policy Link is on the site that displays the forms users complete.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
Information provided is at will.

7.2: What are the procedures that allow individuals to access their information?
Once forms are submitted, it cannot be accessed

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.

GSA has developed, implemented, and regularly update annual training modules on IT Security and Privacy Awareness and Sharing Securely in a Collaborative Environment. All GSA account holders also electronically sign the GSA Rules of Behavior.

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?

The Security and Privacy Training provided on an annually basis covers the overall process.

The System Owner ensures that all users follow the account access request and approval process to grant access to the application.