

Privacy Impact Assessment

Challenge.gov

June 8, 2018

**Privacy Impact Assessment (PIA) for the
Technology Transformation Service (TTS)**

CHALLENGE.GOV

June 8, 2018

**Contact Point:
Joseph Hoyt
Technology Transformation Service (TTS)
GSA IT – Staff Office ISSO Support Branch
202.969-7181**



Abstract

Challenge.gov is an Office of Technology Transformation Service (TTS) application. The Challenge.gov platform is available at no cost for federal agencies to host crowdsourcing competitions. The PIA is required to be completed and reviewed annually or when there are significant changes to the system or a change in the privacy posture in accordance with the GSA IT Security Policy 2100.1.

Overview

The Challenge.gov platform is a listing of challenge and prize competitions, all of which are run by more than 100 agencies across the Federal government. These include technical, scientific, ideation and creative competitions in which the U.S. government seeks innovative solutions from the public, bringing the best ideas and talent together to solve mission-centric problems. At a minimum, users submitting challenge solutions are required to provide an e-mail address, username and password, by their own designation. In addition, users may voluntarily elect to provide the following data elements, though none are required for participation:

- First and last name
- Phone number
- City, state and country
- Website (e.g., school, company, Twitter or LinkedIN pages)
- Photo or image
- Biographical sketch of no more than 1,000 words
- Additional skills and interests from a preset selection
- Additional skills and images in a free form text box

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the application in question?

The specific legal authority to collect data for Challenge.gov comes from OMB M-10-11, "Guidance on the Use of Challenges and Prizes to Promote Open Government"
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-11.pdf>

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

The required information collected by Challenge.gov, which are email addresses, is not Privacy Act System of Records; therefore a SORN is not required. In addition, the optional information collected (first/last names, phone number, and city/state/country) is also excluded.

1.3 Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

A 1 Year LATO SSP has been completed for Challenge.gov. The system was granted its Limited Authority to Operate (ATO) on September 26, 2017 as a Moderate system under the Federal Information Processing Standards Publication 199.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. The list of challenge and prize competitions is managed by each agency that submits them.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected by Challenge.gov is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the application collects, uses, disseminates, or maintains.

At a minimum, users submitting challenge solutions are required to provide an e-mail address, username and password, by their own designation. In addition, users may voluntarily elect to provide the following data elements to create a profile, though none are required for participation:

- First and last name
- Phone number
- City, state and country
- Website (e.g., school, company, Twitter or LinkedIn pages)
- Photo or image
- Biographical sketch of no more than 1,000 words
- Additional skills and interests from a preset selection
- Additional skills and images in a free form text box

2.2 What are the sources of the information and how is the information collected for the application?

All users have the option to register on Challenge.gov by creating a user account and profile to submit a solution. The user inputs this information directly and samples of the registration forms are below.

Federal Challenge Managers Only: You must use an OMB MAX Information System account to access this platform. Register for OMB MAX or, if you already have an account, log in to Challenge.gov.

Solvers, Inventors, Entrepreneurs, and Fans: Complete the fields below to register or submit your solutions to Challenge.gov.

* Username (required)

First Name (optional)

Last Name (optional)

Next

Already have an account? [Log in](#)

There is no cost for the public to participate in the Challenge Program.

* E-mail (required)

* Password (required)

* Confirm Password (required)

Password Requirements

Use at least 8 characters
Use a mixture of upper and lower case characters
Use numbers
Use special characters such as ! " ? \$ % ^ &)

Have a password created for you

1. Define length of password
16 characters (at least 8)

OR

2. Choose your password
r{dpx25h}2d\$%Cb2

Opt out of receiving news and information (e.g., newsletters) from Challenge.gov.

By creating an account, you agree to our [Terms of Service](#) and [Privacy Policy](#), and acknowledge that your username cannot be modified.

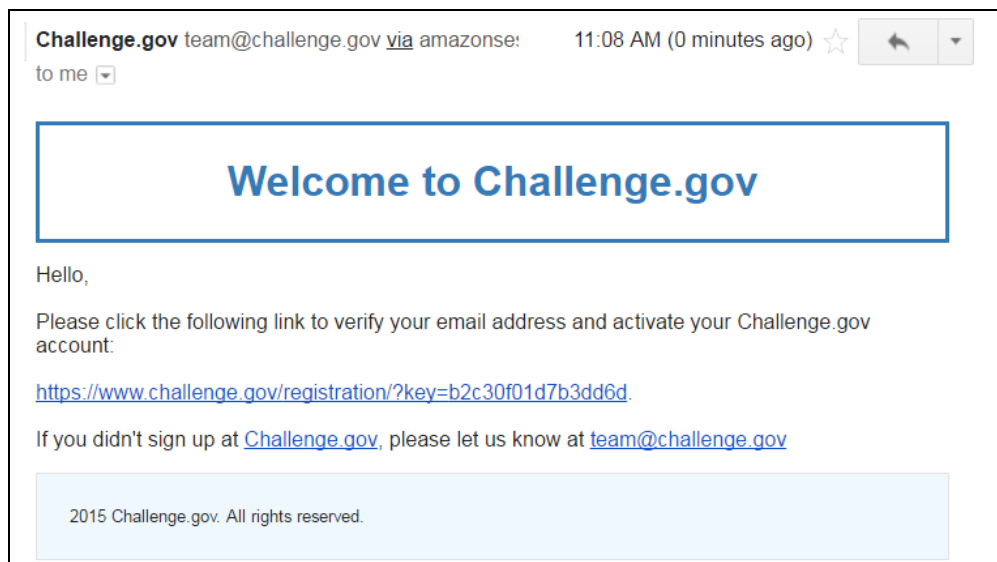
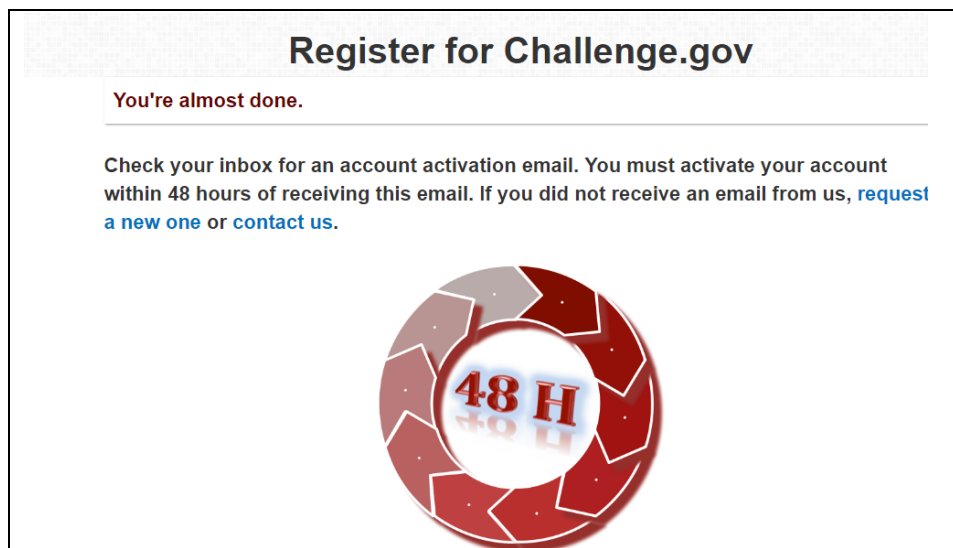
Register

2.3 Does the application use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system uses information provided directly from the user. Challenge.gov does not use information from commercial sources.

2.4 Discuss how accuracy of the data is ensured.

Users of Challenge.gov are responsible for accurately submitting their information. E-mail addresses are verified for complete format only. Before a user is permitted to use the platform, an auto-generated e-mail will be sent to the email provided at registration. Users must click the embedded link, or cut and paste the link into a browser window, to verify a working e-mail address and ownership before a user account is activated. See the screenshots below:



2.5 Privacy Impact Analysis: Related to Characterization of the Information

The data collected by the system adheres to the Principle of Individual Participation because it is collected directly from the user. The identifiable information collected is optional (excluding email addresses) and privacy risks are minimal. The system itself captures email addresses, names, phone numbers, and city/state/country, and is only viewable if the user opts-in within the update profile module to display their information to the public. See the screenshot below:

The screenshot shows a user profile update form with the following sections and fields:

- Profile Visibility:** Radio buttons for Make Profile Public and Make Profile Private.
- Name:**
 - Profile Display Name: acampbell
 - First Name: Akisha
 - Last Name: Campbell
- Contact Information:**
 - Email: * akishacampbell4505@gmail.com
 - Website: [Empty field]
 - Phone Number: [Empty field]
- About Yourself:**
 - Location: <-- Select Country --> [Dropdown menu]
 - City: [Empty field]
 - Biographical Info: [Text area, 1000 character limit]

Privacy options for each field are shown as radio buttons: Show on public profile and Don't show on public profile. Red circles highlight the "Make Profile Private" option at the top and the "Don't show on public profile" options for the Name, Contact, and About Yourself sections.

Section 3.0 Uses of the Information

The following questions require a clear description of the application's use of information.

3.1 Describe how and why the application uses the information.

At a minimum, users submitting challenge solutions are required to provide an e-mail address, username and password, by their own designation. In addition, users may voluntarily elect to provide the following data elements to create a profile, though none are required for participation:

- First and last name

- Phone number
- City, state and country
- Website (e.g., school, company, Twitter or LinkedIN pages)
- Photo or image
- Biographical sketch of no more than 1,000 words
- Additional skills and interests from a preset selection
- Additional skills and images in a free form text box

E-mail addresses are verified for complete format only. Before a user is permitted to use the platform, an auto-generated e-mail will be sent to the email provided at registration. Users must click the embedded link, or cut and paste the link into a browser window, to verify a working e-mail address and ownership before a user account is activated.

3.2 Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

The application does not use technology to conduct electronic searches or queries within a database to discover predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

Role	Internal or External	Sensitivity Level	Authorized Privileges and Functions Performed
Site Admin	Internal	Moderate	<ul style="list-style-type: none"> ● Maintains access to all content ● Maintains access to the back-end admin dashboard (i.e., modify the WordPress configuration for the site) ● View/approve/publish challenges in draft form ● Generate alerts to public solvers ● Publish to the PrizeWire blog ● Add/modify/delete challenges, agency information, and user accounts ● Add/modify individual agency page content ● Add/modify individual agency challenge content ● Review, edit and download “hidden” submissions ● Manage discussion boards and comments ● Correspond with users through the application ● Read publicly available web site content (i.e., view challenges) ● Create and manage their own individual user profiles ● Post in discussion boards
Agency User	External	Moderate	<ul style="list-style-type: none"> ● Add/modify individual agency page content ● Add/modify individual agency challenge content ● Review, edit and download “hidden” submissions ● Manage discussion boards and comments ● Correspond with users through the application ● Read publicly available web site content (i.e., view challenges) ● Create and manage their own

Role	Internal or External	Sensitivity Level	Authorized Privileges and Functions Performed
			individual user profiles <ul style="list-style-type: none"> ● Post in discussion boards
Public User	External	Low	<ul style="list-style-type: none"> ● Register to create/manage individual profile ● Read publicly available web site content (i.e., view challenges) ● Submit solutions ● Post in discussion boards
Subscriber	External	Not Applicable	<ul style="list-style-type: none"> ● Read publicly available web site content (i.e., view challenges) ● Post in discussion boards

3.4 Privacy Impact Analysis: Related to the Uses of Information

The only identifiable information collected by the general public is optional excluding their email address. If identifiable information is voluntarily provided, it is included in the user's profile which is hidden from public display by default (unless specified by the user – See Question 2.5); it is very rare that public participants actually build out their profiles and make them visible to the public.

In addition, Application Administrators have access to all application data.

Section 4.0 Notice

The following questions seek information about the application's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the application provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

A privacy statement is displayed which states:

The system does not collect personal information for any purpose other than to respond to the user and provide information for which the user opted-in (for example, to respond to their questions via email). The application shares information the user provides with another government agency if your question relates to that agency, or as otherwise required by law.

The privacy statement is located here: <https://www.challenge.gov/privacy-policy/>

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

On the registration page, a user must agree to abide by the Terms of Service and Privacy Policy of Challenge.gov. If they agree with the terms, they would then select the "Register" link on the bottom of the registration page in order to receive an account.

4.3 Privacy Impact Analysis: Related to Notice

Challenge.gov follows the Principle of Transparency and provides the user with sufficient information to determine whether or not they wish to provide their personal data.

Section 5.0 Data Retention by the application

The following questions are intended to outline how long the application retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

If a user provides identifiable information for their profile, this information is retained in the system indefinitely unless either 1.) the user's account is inactive more than 365 days, at which time, the user's account is deleted; or 2) the user deletes their account, which they could do at any time via the platform's online interface. The retained data is only accessible by application administrators and the public (if the user has accepted the option to make their profile public (See the screenshot in Question 2.5)).

5.2 Privacy Impact Analysis: Related to Retention

The names and contact information provided voluntarily by users are retained in connection with each challenge and in order to provide a direct response to the user from challenge.gov or the agency responsible for the challenge in question. The information is currently retained indefinitely for active accounts unless accounts are inactive for more than 365 days, at which time the account is deleted by the Challenge.gov PMO, or a user deletes his/her own account.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Identifiable information collected within Challenge.gov is shared with the appropriate agencies. For example, if a user has a question regarding a challenge, the agency associated with that challenge could respond directly to that individual. In addition, in instances where a citizen wins a challenge and is thus entitled to a financial prize or other tangible reward, the agency sponsoring that challenge may contact the user directly via Challenge.gov to offer necessary guidance on separate channels for providing personal information to verify eligibility and/or receive payment (e.g., address or bank account number). Challenge.gov does not collect or provide this information. In these cases, it is the sole responsibility of the agency or agencies sponsoring the challenge to ensure proper safeguards around the collection and retention of that personal information.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As discussed above, Challenge.gov is not a System of Records for Privacy Act purposes.

6.3 Does the application place limitations on re-dissemination?

Contact information is not provided to agencies; instead, agencies are encouraged to use the application's discussion board and/or correspondence feature to contact public participants directly.

6.4 Describe how the application maintains a record of any disclosures outside of the Agency.

N/A

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Email addresses, names, and phone numbers are excluded from disclosure under FOIA.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Any information inputted by the general public can be edited excluding username.

7.3 How does the application notify individuals about the procedures for correcting their information?

There is no notice sent to the user concerning procedures for correcting their personal identifiable information within the system.

7.4 Privacy Impact Analysis: Related to Redress

If any data, such as a user's name or phone number was submitted inaccurately, the risk would be minimal because this data is only used by agencies to directly contact the user in order to address their comment and/or question and award challenges. However, the email address is validated as an active account so that information is actually verified. Therefore if the phone number provided is inaccurate, the user can always be contacted via email.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the application ensure that the information is used in accordance with stated practices in this PIA?

Outside of the site administrator role, all other roles can see only their own user account information that was voluntarily provided by a.) users who voluntarily make their profile information public, or b.) users who provide their information directly to the agency. By default, agency users who are validated through the secure OMB MAX website may only see usernames associated with their agency challenge submissions. The platform also limits agency users from updating challenges outside their department or agency component to safeguard the integrity of the institution or organization.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the application.

GSA provides mandatory annual privacy and security training.

8.3 What procedures are in place to determine which users may access the information and how does the application determines who has access?

Agencies do not have access to public participant information, unless the solver specifically provides contact details in a submission. Only the Challenge.gov Program Office and contracted development vendors can access the solver database on the back-end, and primarily to assist the public with login and submission (e.g., resetting passwords, confirming submissions, etc.).

8.4 How does the application review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within GSA and outside?

There are no information sharing agreements. The Privacy Policy that must be agreed to prior to registering for an account states:

We do not collect personal information for any purpose other than to respond to you and provide information for which you've opted-in (for example, to respond to your questions via email). We only share the information you give us with another government agency if your question relates to that agency, or as otherwise required by law.

