

**PRIVACY IMPACT ASSESSMENT**

Challenge.gov Government-wide Challenge Platform

November 2011

Prepared by:

Office of Citizen Services (OCS-SC)

General Services Administration

|  |  |
| --- | --- |
|  | **Explanation/Instructions** |
|  | In order to participate in a challenge, the public must register a user account.  This can be accomplished by creating a user account based on their e-mail address and a password that they create, as well as a username, first and last name, and location (free-form text box; the platform does not perform any automated geolocation of users in relation to their user profiles).  They may also optionally upload an image that will be publicly associated with their user profile; if they choose to upload an image, there is no requirement that the image include a photograph of the citizen registering, or of any other particular content.  Users will also be able to fill out their profile with other information down the road, including their company name or even links they want to display to their Twitter or homepage.  Users will have the option of making this information part of their public profile.  The site will provide a disclaimer in the privacy statement attesting to the fact that this is not a privacy act system of record, submission of this data is voluntary, and that any PII collected by the system is being done so purely for the purposes of authentication.  Moreover, the information is collected in databases owned by a third party, ChallengePost, and will never be made available to the government except in cases where:   * A user provides an explicit request/permission to have that information accessed.      * The information is required for law enforcement purposes or by statute.     The privacy statement will further commit to providing users at least 30 days of advance notice should there be a change to any of these policies.  A confirming e-mail will be sent from the system to the citizen before they can participate in any challenge or follow challenges through their user profile.  This step is included as a spam reduction measure and is common on web-based social collaboration platforms.  This is a public challenge platform in which citizens’ interactions with challenges will be posted publicly in chronological order.  The following profile data entered by a user is made visible by default to all participants in the site:   * Username * Location (free-form text box) * Profile image (if supplied)   Additionally, users will be identified publicly by their full first and last name, as entered by them on the registration form, if and only if they opt in to do so by checking a box as part of the registration/login process.  This option will be turned off by default, and can be undone later even after being initially enabled.  Citizens can interact with challenges in two ways:   * “Following” or supporting a challenge, in which a citizen is publicly recognized as a supporter of the challenge, and opts in to receive periodic e-mail updates about the challenge; and      * Solving a challenge, in which a citizen submits a solution to a challenge that is posed by an agency.   ***"Following"/Supporting a Challenge***  Supporters of a challenge do not have to be registered users; if they click to support a challenge and are not logged in, the number of supporters will increase even if they then decline to create an account. The "support" number will not be attributed to that user unless they create an account during that session, which they will be offered the opportunity to do.   ***Solving a Challenge***  In addition to supporting challenges, citizens can interact by proposing solutions to challenges, i.e. acting as a solver.  Depending on the type of challenge, solvers may submit text, upload a file, or provide link(s) to an external resource.  The content of submissions is entirely at the discretion of the solver, and it is the solver’s responsibility to avoid submitting PII as part of their solution.  However, agencies will have the ability to moderate solution submissions should it be required.  Also, depending on the type of challenge, challenge posters can decide to ask solvers to submit additional information such as a contact phone number and company.  This information will be available only to System Administrators (ChallengePost) and to the government staff sponsoring the challenge.  If this includes any PII, it will be the responsibility of the agency sponsoring the challenge to ensure that the privacy of that information is protected.  ***Google Analytics***  The Challenge.gov platform will use a Google Analytics tool to gain data about traffic to the site.  This information will be collected through the use of persistent cookies.  These cookies will never collect any information about a visitor that could be considered PII, and therefore are considered a Tier 2 use of web measurement and customization technologies, as defined by OMB M-10-22.  All traffic data collected through Google Analytics is reported in the aggregate and anonymously, and cannot be associated with any individual user who has registered on the Challenge.gov site.  Some cookies may be stored for up to two years.  ***KISSmetrics***  Challenge.gov uses KISSmetrics to study funnels - anonymous analytics around user experience. Challenge.gov does not pass any PII about users to KISSmetrics.  In addition, KISSmetrics:  -does not use ETags or any other persistent cookie for tracking.  -has never shared any information about a user with any third party.  -does not track users across different websites, nor does it have the ability to do so.  -has added a consumer-level opt-out for those who wish to be entirely removed from all KISSmetrics tracking.  ***Exporting and Use of Data***  E-mail information is used for authentication purposes only, which does not require exporting it.  Registrants' responses to the "location" question, which takes the form of unverified free-form text, may be analyzed for the purpose of determining, in aggregate, the geographic areas from which users are registering and solutions are being submitted.    No PII collected through the basic input mechanisms in this platform is stored or retrieved by the U.S. government.  It is stored in a database owned by the System Administrator of the site, ChallengePost.  ChallengePost will not retrieve or view non-public PII submitted by registrants except under the circumstances spelled out earlier in this document: Explicit request or permission to do so, including as indicated by opting in via a checkbox; necessity for law enforcement purposes; or statutory requirement.  In general, contact between users of the platform—supporters, solvers, judges, challenge sponsors, and administrators—will be made through a web-based form interface that enables e-mails to be sent without revealing the e-mail address of the sender to the recipient(s), or of the recipient(s) to the sender.   The procedure for submitting solutions will include the requirement that submitters state that they have read and agree to be bound by the Official Terms and Conditions of that challenge, which are set on the basis of individual challenges.  This fact will be spelled out in the site's privacy policy/notice.  The privacy notice for the public will reflect these facts as they pertain to the public's use of the site. |
|  | Government employees have the ability to use the platform to submit challenges.  They use the same registration process as general citizens, and thus are subject to the same information collection.  However, as with the information above, the information is stored in databases that are not owned by the government, and thus the information is not made available to the government except in the circumstances described above. |
|  |  |

**PART II. SYSTEM ASSESSMENT**

**A. Data in the System**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1.  Describe all information to be included in the system, including personal data. | a. The tool is a Software as a Service (SaaS) vendor offering hosted outside the GSA infrastructure, on the Amazon EC2 cloud.  It will serve multiple agencies by offering a platform for agencies to pose challenges to citizens and solicit solutions and support for those challenges. Data will include proposed solutions (text, uploaded file, or link(s) to resources), votes/ratings of individual solutions, and open interactive discussion by citizens.  b. E-mail address submitted by the citizen visiting the site, to be used as a login, along with username, first name, last name, location (free-form text box), and optional profile image.  E-mail addresses are collected for authentication purposes only.  First and last names may be displayed publicly with a registrant's express consent.  All of this information may be retrieved if consent is provided, or as require for law enforcement purposes or by statute.  c. In addition, participants can submit an image associated with their profile, which may contain a photograph of themselves, or any other content they choose.  Also in the future, users will be provided with the opportunity to fill in additional profile fields, which they will have the option of making part of their public profile. |
| 1. a.  What stage of the life cycle is the system currently in? | Design/Planning |
| 2. a.  What are the sources of the information in the system? | All information in the system is provided by participants as they register for the system and interact with challenges. |
| 2. b.  What GSA files and databases are used? | None |
| 2. c.  What Federal agencies are providing data for use in the system? | None; however, agencies may use the platform to run challenges based on the use of agency data.  This will only ever involve datasets that have already been approved for public release by the agency. |
| 2. d.  What State and local agencies are providing data for use in the system? | None |
| 2. e.  What other third party sources will the data be collected from? | None. |
| 2. f.  What information will be collected from the individual whose record is in the system? | E-mail, username, first name, last name, location (free-form text), and optional profile image.  Other fields may be added in the future; displaying them publicly will be optional for the user.  The individual may also submit solutions, comments, votes, or other feedback in response to challenges posted, at the individual's discretion. |
| 3. a.  How will the data collected from sources other than Federal agency records or the individual be verified for accuracy? | It is a tool made available for voluntary use.  Visiting citizens will be responsible for accurately submitting their information.  Other fields may be added in the future; displaying them publicly will be optional for the user.  E-mail addresses will be verified for complete format only. Before access is permitted, a return e-mail will be sent to verify that the e-mail address is a functioning e-mail address and is in fact owned by the user who performed the registration process.  In instances when a website user wins a challenge and is thus entitled to a financial prize or other tangible reward, the agency sponsoring that challenge may ask the user to provide personal information necessary to make payment, such as an address or bank account number.  This information is provided at the discretion of the user. In these cases, it is the sole responsibility of the agency or agencies sponsoring the challenge to ensure proper safeguards exist around their collection and retention of that personal information. |
| 3. b.  How will data be checked for completeness? | E-mails will be verified for complete format only. Before access is permitted a return e-mail will be sent to verify that the e-mail address is a functioning e-mail address.  This is a spam reduction measure. |
| 3. c.  Is the data current?  How do you know? | It is a tool made available for voluntary use.  Visiting participants will be responsible for accurately submitting an e-mail address.  Before access is permitted, a return e-mail will be sent to verify that the e-mail address is a functioning e-mail address and is in fact owned by the user who performed the registration process.  This is a spam reduction measure. |
| 4.  Are the data elements described in detail and documented?  If yes, what is the name of the document? | The privacy statement will display messaging confirming to the visiting user the limited use of the e-mail for authentication purposes.  The privacy policy will also indicate that providing a profile image that includes one’s own photograph is voluntary on an opt-in basis and that, when making comments, the registrant's username will be displayed publicly by default, and will only be accompanied by their first and last name, as submitted, with their express consent via an opt-in checkbox.  Furthermore, the policy will clearly state that this is not a privacy act system of record (see Question 1). |

**B. Access to the Data**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1. a.   Who will have access to the data in the system? | All users and the general public will have access to the challenges submitted, discussion, and votes associated with each challenge, as well as the limited profile information voluntarily submitted by each participant, as this is a public platform intended for transparent uses.  Challenge administrators can delete inappropriate comments or solutions.  Challenge posters will have discretion over which solutions become viewable by the public and when they do so, on a per-solution basis. |
| 1. b.  Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)?  If yes, explain the policy and rationale supporting this decision. | E-mail addresses, usernames, first name, last name, location, and profile images are excluded from disclosure under FOIA. |
| 2.  How is access to the data by a user determined?  Are criteria, procedures, controls, and responsibilities regarding access documented? | Access to data is determined by user roles, including:   * Content Administrators (GSA), and System Administrators/Developers of Code (ChallengePost)      * Vendor Associates      * Federal employees who administer challenges or department/agency pages      * Citizens using the platform, or contest judges who are non-federal employees   For the latter two groups, controls on data are implemented automatically through the platform's permissioning scheme.  For the first two, GSA/OCS will retain responsibility for ensuring controls on information as work is performed and the platform operates.  User roles and permissions will be documented. |
| 3.  Will users have access to all data in the system or will the user's access be restricted?  Explain. | * **Individual Access**:  The only data collected is voluntarily.  Users' username, and first and last name if they so choose, are visible to the public, and this is highlighted in the privacy policy provided to the public on the web site.  In many cases where this identifier for a user is displayed, clicking it may display that user's full profile, including location (free-form text), and optional profile image.  This information may also potentially be displayed on other sites that pull public feeds of information from Challenge.gov, i.e. through RSS or an API.      * **Content Administrators (GSA) and System Administrators/Developers of Code** **(ChallengePost)** have access to data as appropriate to fulfill their roles, within the conditions spelled out in this PIA and the site's privacy policy.  As content administrators, the government does not own the database in which registrants' information will reside.      * **Vendor Associates’** access to the system is controlled by the vendor and is dictated by duties and requirements of their positions and by the terms of the service agreement.      * **Federal employees who administer challenges or department/agency pages** have access to all information that is made public.  They may also have access to anonymous Google Analytics traffic data for the challenge pages which they respectively administer.      * **Citizens using the platform** will have access only to information that is made public. |
| 4.  What controls are in place to prevent the misuse (e.g. browsing) of data by those having access? | ChallengePost and Vendor Associates are operating under the same rules of behavior described in the ChallengePost privacy policy in terms of protecting the privacy of others and not using information in the system for personal gain or to the benefit of others.  Passwords and segmentation of function provide adequate protections. |
| 5. a.  Do other systems share data or have access to data in this system?  If yes, explain. | No other system has access to this data, other than Google Analytics, which has access only to the anonymized, aggregate analytics data which it retrieves from cookies.  Some cookies may be stored for up to two years.  Other systems will also be able to pull data from this system via an API, but that API will only feed data that is already publicly available (i.e., no PII). |
| 5. b.  Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface? | Not applicable |
| 6. a.  Will other agencies share data or have access to data in this system (International, Federal, State, Local, other)? | Other federal agencies will host their challenges on the Challenge.gov platform. |
| 6. b.  How will the data be used by the agency? | The information will not be used by the Agency.  The service provider’s tool uses e-mail addresses only as a means of authenticating a user of the challenge platform.  Location responses may be used to aggregate responses for purposes of metrics (such as number of responses from various regions of the country). |
| 6. c.  Who is responsible for assuring proper use of the data? | The Program Manager |
| 6. d.  How will the system ensure that agencies only get the information they are entitled to? | Not applicable.  Note:  All comments are public.  E-mail addresses are used only for authentication purposes, except where access is explicitly authorized, required for law enforcement reasons, or mandated by statute. |
| 7.  What is the life expectancy of the data? | The challenge tool retains users' registration details permanently, unless the user deletes their account, which they may do at any time via the platform's online interface.  This is a standard feature of websites in which the creation of a unique, persistent user account is a requirement for participation. |
| 8.  How will the data be disposed of when it is no longer needed? | The program will retain users' registration details permanently, unless the user deletes their account, which they may do at any time via the platform's online interface.  This is a standard feature of websites in which the creation of a unique, persistent user account is a requirement for participation.  The system provides for the export of challenge data (i.e., the submissions received in response to a challenge) in various formats for purposes of records management. |

**C. Attributes of the Data**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1.  Is the use of the data both relevant and necessary to the purpose for which the system is being designed? | Yes.  E-mail addresses are necessary to authenticate a user of the challenge platform, to allow users to return and modify their information and ideas, to control the number of times a user can vote on a solution or follow a challenge, and to discourage frivolous participation.  Upon initial log-in, an e-mail is sent back to the email address to confirm the e-mail address is working before allowing participation.  This is a spam prevention measure. |
| 2. a.  Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? | No |
| 2. b.  Will the new data be placed in the individual's record (client or employee)? | No |
| 2. c.  Can the system make determinations about individuals that would not be possible without the new data? | No |
| 2. d.  How will the new data be verified for and accuracy? | E-mails will be verified for complete format only. |
| 3. a.  If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access?  Explain. | Data is not being consolidated.  Location data may be used to aggregate metrics (such as responses from which regions of the country).  Only System Administrators have download capabilities and no PII submitted by users will be viewed, retrieved, or exported without their explicit permission or as required for law enforcement purposes or by statute. |
| 3. b.  If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?  Explain. | Processes are not being consolidated. |
| 4.  How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain. | Data containing PII submitted by users cannot be retrieved by the government. The system will retrieve registrants' records by username, which is a manufactured alias and does not constitute PII. (Registrants are responsible for omitting PII from this field.) |
| 5.  What are the potential effects on the privacy rights of individuals of:  a.  Consolidation and linkage of files and systems;  b.  Derivation of data;  c.  Accelerated information processing and decision      making; and  d. Use of new technologies.  How are the effects to be mitigated? | There are no known effects on the due process rights of individuals who avail themselves of the tool.  This system is not linked to other files and systems.    Participants will be presented with a clear disclaimer in the Privacy Policy that any submissions of e-mail addresses, first and last name, or location are voluntary and that this is not a privacy act system of record. |

**D. Maintenance of Administrative Controls**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1. a.  Explain how the system and its use will ensure equitable treatment of individuals. | There are no known effects on the equitable treatment of individuals who avail themselves of the challenge tool.  This system is not linked to other files and systems. |
| 1. b.  If the system is operated in more than one site, how will consistent use of the system be maintained at all sites? | The system is designed to provide separate challenge pages for each agency, but a standard account template is developed and applied by GSA to each challenge site established. |
| 1. c.  Explain any possibility of disparate treatment of individuals or groups. | There is no possibility of disparate treatment of individuals. |
| 2. a.  What are the retention periods of data in this system? | The program will retain users' registration details indefinitely unless the user deletes their account, which they may do at any time via the platform's online interface.  This is a standard feature of websites in which the creation of a unique, persistent user account is a requirement for participation.  Other information (comments, solutions, votes) will be retained until the site is decommissioned. |
| 2. b.  What are the procedures for eliminating the data at the end of the retention period?  Where are the procedures documented? | Registration data will not be eliminated except voluntarily by the user who originally submitted it, which they may do at any time via the platform's online interface.  This is a standard feature of websites in which the creation of a unique, persistent user account is a requirement for participation.  Participation data will not be eliminated. |
| 2. c.  While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations? | The individual will be responsible for ensuring that the information is complete, accurate, and up-to-date when they first use the tool via authentication of a valid e-mail address.  Thereafter, they may keep aspects of their user profile current via the platform's online interface. |
| 3. a.  Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)? | No.  Although this particular platform is new, the technologies that support it are all previously established in government and have been used for similar purposes. |
| 3. b.  How does the use of this technology affect individuals’ privacy? | No effect on individual privacy.  The only impact is the storage of an e-mail address and name.  The e-mail address is submitted voluntarily for authentication purposes only, and after being provided with appropriate notices on the web site.  The name is not displayed publicly without individuals' explicit permission.  In addition, the persistent cookies used by this site do not collect or store any PII, nor can they be used to track individual users' activities across other websites other than those within Challenge.gov.  Google Analytics provides reporting on "referring sites" but this data is only recorded anonymously and reported in the aggregate.  Some cookies may be stored for up to two years. |
| 4. a.  Will this system provide the capability to identify, locate, and monitor individuals?  If yes, explain. | No.  Individuals are asked to provide "location" but this is a free-form text box.  It can contain any level of specificity (e.g., "Minnesota" or "the Earth"), and is not independently verified.  No individual visitor's activities, on or off this website, can be specifically monitored. |
| 4. b.  Will this system provide the capability to identify, locate, and monitor groups of people?  If yes, explain. | No |
| 4. c.  What controls will be used to prevent unauthorized monitoring? | The information that would be required for such monitoring is never solicited or entered into the system. |
| 5. a.  Under which Privacy Act System of Records notice (SOR) does the system operate?  Provide number and name. | This challenge platform tool is not a System of Record.  The sole purpose is to establish a mechanism for citizens to browse, support, discuss, and solve challenges posed publicly by agencies.  No information is retrieved by a unique identifier and so this database does not meet the definition of a System of Record. |
| 5. b.  If the system is being modified, will the SOR require amendment or revision? Explain. | Not applicable; new system. |