Adapted Privacy Impact Assessment

crowdSPRING

March 14, 2012

Contact

Departmental Privacy Office
U.S. Department of the Interior
1849 C St, NW
Mail Stop MIB-7456
Washington, DC 20240
(202) 208-1605
DOI_Privacy@ios.doi.gov

One PIA may be prepared to cover multiple websites or applications that are functionally comparable as long as agency or bureau practices are substantially similar across each website or application. However, any use of a third-party website or application that raises distinct privacy risks requires a complete PIA exclusive to the specific website or application. Department-wide PIAs must be elevated to the OCIO for review and approval.

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

The crowdSPRING application is a U.S. owned crowdsourced creative service used by thousands of users world-wide that provides a platform and user base for the public to submit design ideas upon the request of an individual, corporate or governmental entity. In crowdSPRING's design request process, one or more winning designs are selected by the design requestor and payment is made to the designer. The crowdSPRING application will provide the Department of the Interior (DOI) with a unique opportunity to reach the design community and the general public for their input with various design requests such as logos, to foster and share ideas, promote public participation and collaboration, and increase government transparency.

Designers who submit designs to DOI through crowdSPRING must be registered crowdSPRING users. User profiles in crowdSPRING include name, nickname, email address, and may include other personal information at the user's discretion, such as mailing address, and profile photograph. Upon completion of a winning design, the designer must provide crowdSPRING with payment information, such as Paypal account or bank wiring information including credit card or bank account numbers. Users of crowdSPRING can communicate with each other and with groups through blogs and forums hosted on the crowdSPRING web site, as well as crowdSPRING's user-to-user messaging system. While DOI can provide submission guidelines for DOI design requests, DOI has no control over content in crowdSPRING except for official DOI postings, including personal information provided by users.

The primary account holder is the Department of the Interior Office of Communications, which will be responsible for ensuring appropriate use of the Department's primary official crowdSPRING page. DOI bureaus and offices are responsible for ensuring appropriate use of their official crowdSPRING pages in accordance with applicable laws, regulations, and DOI policies.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities that authorize the use of the third-party website or application?

Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; the

Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 U.S.C. 1401; OMB Circular A-130; 210 Departmental Manual 18; 110 Departmental Manual 5.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

Generally, members of the public can browse the crowdSPRING site without registering or providing PII. However, to participate in the service users are required to register with crowdSPRING. User accounts are password protected and contain contact information and other personal information, such as name, nickname, email address, physical contact information, and may contain financial information, such as credit card or bank account numbers, transactional information, project entries, and content of chats, blogs or correspondence. Also, crowdSPRING may collect web log information such as IP address, statistics on page views and traffic to and from the crowdSPRING site.

PII submitted by users to crowdSPRING will not be transferred to DOI. The only information that may become available to DOI includes name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, which are submitted or posted by users during design projects. Users can control access to their account information, and access to users' contact information is limited to other users involved in a transaction when a project winner is selected. DOI does not collect, maintain or disseminate any PII when making payments to designers, as crowdSPRING serves as a payment conduit between the design requestor and the successful designer.

There may be unusual circumstances where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, nickname, email address, project entries, feedback, ratings and contents of comments, blogs or correspondence, and may be used to notify the appropriate agency officials or law enforcement organizations.

In some instances DOI may also receive correspondence or entries via email from members of the public who do not wish to use the crowdSPRING service. This correspondence may contain a name and personal email address at a minimum, and may also contain other personal information and content of the communication. These records will be maintained in accordance with DOI-08, Social Networks system of records notice, or other applicable bureau or office system of records notice. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

2.2 What are the sources of the PII?

Sources of information are crowdSPRING users world-wide, including members of the general public and Federal employees, and may include other government agencies and private organizations.

2.3 Will the PII be collected and maintained by the agency?

If a crowdSPRING user or member of the public interacts with DOI through its official crowdSPRING page, submits a design, posts comments, requests information or submits feedback from their use of crowdSPRING, their name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, and other personal information may become available and used to communicate or provide requested information to the user.

Also, there may be unusual circumstances where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

DOI may also receive correspondence or entries via email from members of the public who do not wish to use the crowdSPRING service. This correspondence may contain a name and personal email address at a minimum, and may also contain other personal information and content of the communication. Any DOI bureau or office that uses crowdSPRING in a way that creates a system of records must complete a separate PIA for the specific use and collection of information, and must maintain the records in accordance with DOI-08, Social Networks system of records notice or other applicable bureau/office system of records notice. DOI Privacy Act system of records notices may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

No, DOI is not using crowdSPRING to survey the public or in any manner that would trigger the requirements of the Paperwork Reduction Act. Specifically, the use of web-based technologies to conduct contests is addressed in a memorandum issued by the Office of Management and Budget dated April 7, 2010, titled, "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act" (http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf). The memorandum states in part, "...contests that permit respondents to create their own submissions are not covered by the PRA if no additional information is collected for the contest beyond what is necessary to contact the entrants."

SECTION 3: The Agency's Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

DOI uses crowdSPRING to foster and share ideas, facilitate feedback on Department programs, promote public participation and collaboration, and increase government transparency. If a crowdSPRING user or member of the public interacts with DOI through its official crowdSPRING page, submits a design, requests information or

submits feedback from their use of crowdSPRING, their name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user may become available to DOI, and may be used to interact or provide the requested information or service. DOI may also receive correspondence or entries via email from members of the public who do not wish to use the crowdSPRING service. This correspondence may contain a name and personal email address at a minimum, and may also contain other personal information and content of the communication, and may be used to communicate, or provide requested information or service.

Also, there may be unusual cases where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

3.2 Provide specific examples of the types of uses to which PII may be subject.

If a crowdSPRING user requests information or submits feedback through crowdSPRING's messaging service, blogs, or forums, the user's name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user may become available and used to communicate with the individual user or provide the requested information. DOI may also receive correspondence or entries via email from members of the public who do not wish to use the crowdSPRING service. This correspondence may contain a name and personal email address at a minimum, and may also contain other personal information and content of the communication, and may be used to communicate, or provide requested information or service.

Also, there may be unusual cases where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or postings, and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

SECTION 4: Sharing or Disclosure of PII

4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

The crowdSPRING application is a third party web site used by members of the public, Federal employees and organizations world-wide, including Federal, Tribal, State and local agencies who may have access to the data posted in crowdSPRING. DOI does not share PII with these other agencies and is not responsible for how they may access or use data posted on crowdSPRING. Users may not access data on other individual

users, and can access their own information via their online registration with passwords and generally will only have access to information about design projects.

However, there may be unusual cases where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. These incidents may include name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

DOI may share information with the Internal Revenue Service (IRS) regarding payment of a project winner when required as part of the IRS's usual tax-assessing and collecting practices.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

Official mission related information posted on crowdSPRING by DOI is reviewed and approved for public dissemination prior to posting so any privacy risks for the unauthorized disclosure of personal data by the Department is mitigated. However, except for official postings, DOI does not control the content or privacy policy on crowdSPRING. There could potentially be thousands of crowdSPRING users who have access to information posted on crowdSPRING, including the general public, Federal employees, private organizations, and Federal, State, Tribal and local agencies.

The crowdSPRING application requires users to provide a username and an email address. Additional personal information is provided at the user's discretion. However, the provision of information and user consent applies only to terms of use for crowdSPRING, and crowdSPRING is responsible for protecting its users' privacy and the security of the data in the application. DOI has no control over access restrictions or procedures in crowdSPRING, or the personal information provided by users. Users can set their own privacy settings to protect their personal information and are subject to crowdSPRING's Privacy Policy and User Agreement.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

Information regarding winning entries and records generated by the bureaus or offices are retained in accordance with normal records management practices for contracting and payment of services rendered for the originating bureau or office or General Records Schedule 3-3a 1b Routine Procurement Files, which are destroyed 3 years after final payment. Records generated by the Department are retained in accordance with Office of the Secretary records schedule 1110.1. These records are cut off at the end of the fiscal year when payment is made and destroyed three years after cutoff.

For other records that may be generated through the use of crowdSPRING, retention periods vary as records are maintained in accordance with the applicable records schedule for each specific type of record maintained by the Department. Records published through crowdSPRING represent public informational releases by the Department, and must be assessed on a case-by-case basis and may be dependent on the originating office, the subject matter and the purpose of the release or project.

Comments and input from the public must be assessed by whether they contribute to decisions or actions made by the government. In such cases where input from the public serves a supporting role, the comments must be preserved as supporting documentation for the decision made.

Approved methods for disposition of records include shredding, burning, tearing, and degaussing in accordance with National Archives and Records Administration guidelines and 384 Departmental Manual 1.

5.2 Was the retention period established to minimize privacy risk?

Retention periods may vary depending on agency requirements and the subject of the records for the DOI bureau or office maintaining the records. In cases where data serves to support agency business, it must be filed with the pertinent records they support and follow the corresponding disposition instructions. Comments used as supporting documentation will utilize the disposition instructions of the records they are filed with.

SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Yes. Privacy and security officials work with the Office of Communications to develop methods for protecting individual privacy and securing PII that becomes available to DOI.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

PII may become available through interactions with users of the crowdSPRING service, to complete a transaction when selecting a project winner, when communicating with members of the public, and corresponding or submitting entries through email as an alternative to using the crowdSPRING service. There may also be unusual cases where user interactions indicate evidence of illegal activity, a threat to the government or the public, or an employee violation of DOI policy. This information may include name, nickname, project entries, feedback, ratings and contents of comments, blogs or correspondence, or other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

In these cases PII is secured in accordance with DOI Privacy Act regulations 43 CFR 2.51 and applicable DOI privacy and security policies. Access to the DOI network is

restricted to authorized users with password authentication controls, the server is located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on official need to know. Other security controls include continuously monitoring threats, rapid response to incidents, and mandatory employee security and privacy training.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

The official information posted on crowdSPRING by DOI has been reviewed and approved for public dissemination so any privacy risk of unauthorized disclosure of personal data by the Department is mitigated. DOI does not have any control over personal information posted by individual crowdSPRING users, including members of the general public and Federal employees. DOI systems do not share data with the crowdSPRING application.

The crowdSPRING application is a private third party website that is independently operated and controls access to user data within its system. Users control access to their own PII, generally via system settings. DOI has the same access as any other user dependent on individual user personal information disclosures and has no control over user content posted in crowdSPRING, except for official DOI postings.

DOI may also accept submissions of project entries from the public via email as an alternative to using the crowdSPRING application. At a minimum, these entries will contain a name and personal email address, and may also contain project entries, content of communications, and other personal information. DOI will not request personal information from the crowdSPRING service or from users; however, DOI has no control over content of blogs, postings, or email submissions by members of the public. DOI has posted a privacy notice on its official crowdSPRING website which informs users that crowdSPRING is a non-government third party application. It also informs users of how DOI handles information that becomes available through user interactions. Users of crowdSPRING are directed to the DOI Privacy Policy for information handling practices.

The crowdSPRING service provider has access to user information and may use data in the system to alert users about new projects and changes to the site, and to analyze usage of the site, customize site content and layout, and improve product and service offerings. DOI does not request this information, does not have system-level access to user information in the crowdSPRING application, and has no control over how crowdSPRING uses information.

7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of third-party website or application?

DOI's Privacy Policy informs the public of how DOI handles personally identifiable information that becomes available through interaction on the DOI official website. The

Privacy Policy also informs the public that DOI has no control over access restrictions or privacy procedures on third party websites, and that individuals are subject to third party social media website privacy and security policies. DOI's linking policy informs the public that they are subject to third party privacy policies when they leave a DOI official website to link to third party social media web sites.

DOI has also posted a privacy notice on its official crowdSPRING website which informs users that crowdSPRING is a non-government third party application. It also informs users of how DOI handles information that becomes available through user interactions. Users of crowdSPRING are directed to the DOI Privacy Policy for information handling practices.

SECTION 8: Creation or Modification of a System of Records

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

Records or correspondence may be generated through interactions with crowdSPRING users during design projects or selection of winners that may include PII. Any DOI bureau or office that creates a system of records from its use of crowdSPRING must maintain the records in accordance with DOI-08, Social Networks system of records notice, which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

8.2 Provide the name and identifier for the Privacy Act system of records.

Any DOI bureau or office that creates a system of records from its use of crowdSPRING must maintain the records in accordance with DOI-08, Social Networks system of records notice which may be viewed at http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.