# Adapted Privacy Impact Assessment

# GitHub

**May 10, 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?

GitHub is a U.S. owned web-based hosting service for software development projects that uses the Git revision control system for the collaborative development of software. Git is a source code revision management and development system that allows distributed programmers to perform software updates and modifications. Software developed using GitHub is open source software (OSS), which is openly available software that can be freely modified and redistributed.

OSS, particularly when combined with an editing system such as Git and a popular hosting site such as GitHub, can have a number of important advantages over traditional means of software development in terms of quality, cost, and development cycle time, including:

- Review of software code, updates and edits by a broad range of programmers, thereby improving software function and reliability.
- Thorough and rapid testing and debugging.
- Timely updates, allowing the software to continually meet user needs and remain current with prevailing trends.

GitHub is currently used by several Federal agencies, including the Department of the Interior (DOI), for the development of various software applications. DOI's use of GitHub promotes public participation and collaboration, and increases government transparency by allowing the public to directly observe and participate in the design and implementation of certain DOI software projects. This enables the public to better understand the software that DOI uses. DOI will benefit from the use of GitHub by obtaining higher quality software with reduced development time and lower development cost.

The primary account holder is the Department of the Interior Office of Communications, which will be responsible for ensuring information posted on the Department's primary official GitHub page is appropriate and approved for public dissemination. DOI bureaus and offices which use GitHub are responsible for ensuring information posted on their official GitHub page is appropriate and approved for public dissemination in accordance with applicable Federal laws, regulations, and DOI privacy, security and social media 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?**

GitHub requires users to register before posting a software project or viewing or editing software code posted by other users. To register, users must provide a username and email address. Users can create an expanded profile that includes a name, username, website URL, company name, location, professional biography, and a profile picture.

DOI can view the profiles of other GitHub users, including users who edit DOI software code posted on GitHub. If a GitHub user or member of the public interacts with DOI through its official GitHub page, including editing DOI software code, their name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user may become available to DOI. DOI does not collect or share PII through its use of GitHub, except in unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

**2.2 What are the sources of the PII?**

Sources of information are GitHub 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?**

DOI does not actively collect, maintain or disseminate PII through its use of GitHub. If a GitHub user or member of the public interacts with DOI through its official GitHub page, including editing DOI software code, their name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user may become available to DOI. Also, there may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy.

This information may include name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

Any DOI bureau or office that uses GitHub 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. 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 GitHub to survey the public or in any manner that would trigger the requirements of the Paperwork Reduction Act.

## 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?

The Department of the Interior uses GitHub to promote public participation and collaboration, and increase government transparency. If a GitHub user or member of the public interacts with DOI through its official GitHub page, including editing DOI software code, their name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user may become available to DOI and be used to interact or communicate with the user, or provide requested services. DOI does not collect or share PII through its use of GitHub, except in unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, username, email address, website URL, company name, location, professional biography, profile picture and 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 GitHub user or member of the public interacts with DOI through its official GitHub page, including editing DOI software code, their name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user may become available to DOI. This information may be used to interact or communicate with the user, or to provide requested services. DOI does not collect or share PII through its use of GitHub, except in unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, username, email address, website URL, company name, location, professional biography, profile picture 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?

GitHub is a third party web site used by millions of individuals and organizations world-wide, including Federal, Tribal, State and local agencies who may have access to the data posted in GitHub. DOI does not collect or share PII with these other agencies and is not responsible for how they may access or use data posted on GitHub. However, there may be unusual cases where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. These incidents may include name, username, email address, website URL, company name, location, professional biography, profile picture and other personal information provided by the user, and may be used to notify the appropriate agency officials or law enforcement organizations.

### 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 GitHub 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 GitHub. There could potentially be millions of GitHub users who have access to information posted on GitHub, including members of the general public, Federal employees, private organizations, and Federal, State, Tribal and local agencies.

GitHub requires users to provide their username and 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 GitHub. DOI has no control over access restrictions or procedures in GitHub, or the personal information provided by users. GitHub is responsible for protecting its users' privacy and the security of users' data. GitHub users are subject to the GitHub Privacy Policy and Terms of Service, and can set their own privacy settings to protect their personal information.

## SECTION 5: Maintenance and Retention of PII

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

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 GitHub represent public informational releases by the Department, and must be assessed on a case-by-case basis depending on the individual/entity releasing the information and the purpose of the release. There is no single records schedule that covers all informational releases to the public at this time.

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 it supports 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.

DOI does not collect, maintain or disseminate PII from GitHub users, except in unusual cases where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or an employee violation of DOI policy. This information may include name, username, email address, website URL, company name, location, professional biography, profile picture and 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, servers are 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 GitHub 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 GitHub users, including members of the general public and Federal employees. DOI systems do not share data with GitHub.

GitHub is a private third party website that is independently operated and controls access to user data within its system. GitHub 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 GitHub, except for official DOI postings.

**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 on 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.

The Department of the Interior has also posted a privacy notice on its official GitHub profile which informs users that GitHub is a non-government third party application. It also informs users on how DOI handles personally identifiable information that becomes available through user interaction. GitHub users 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?**

No. DOI does not collect, maintain or disseminate PII through its use of GitHub. Any DOI bureau or office that creates a system of records from the use of GitHub will complete a separate PIA for that specific use and collection of information, and 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.**

DOI does not collect, maintain or disseminate PII obtained from the use of GitHub. Any DOI bureau or office that creates a system of records from use of GitHub will complete a separate PIA for that specific use and collection of information, and 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.