EPA United States Environmental Protection Agency

SP11

PRIVACY IMPACT ASSESSMENT

Submit in *Word format* electronically to: Judy Earle (hutt.judy@epa.gov)

Office of Environmental Information

System Name: FOIAonline – Google Analytics

Preparer: Tim Crawford	**Office: OIC/OEI**
Date: May 12, 2016	**Phone: 202-566-1574**

Reason for Submittal: New PIA____ Revised PIA___X_ Annual Review____

This project is in the following life cycle stage(s): Operations and Maintenance

Definition ☐ Development/Acquisition ☐ Implementation ☐

Operation & Maintenance X☐ Termination/Decommissioned ☐

Note: Existing Systems require an updated PIA when there is a significant modification or where changes have been made to the system that may create a new privacy risk. For a listing of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f) at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.aspx

I. Data in the System

1. What data elements will be collected/contained in the system?
   A copy of each Freedom of Information Act (FOIA) request received by the EPA and a copy of all correspondence related to the request, including an individuals' names, mailing addresses, e-mail addresses, phone numbers, and in some cases Social Security Numbers, Dates of Birth, Alias(es) used by the requester, Alien Numbers assigned to travelers crossing national borders, requesters' parents' names, Usernames and Passwords for registered users, FOIA tracking numbers, dates requests are submitted and received, related appeals and agency responses. Records also include communications with requesters, internal FOIA administration documents (e.g., billing invoices) and responsive records.

   FOIAonline will use Google Analytics to collect information about how the site is being used in order to inform future improvements to the site. Google Analytics does this by gathering feedback using non-identifiable aggregated data such as number of unique visitors to a page and the navigation the visitor took to get to a specific piece of content. The Agency will use this data to make modifications to the website to improve the user experience and monitor the traffic on the website.

? persistent

In order to use this tool, Google sets a cookie on your machine or device. While this cookie is set automatically, you may chose not to have the cookie placed on your machine or device without any modifications to the appearance or functionality of the website by following the instructions below. You may also delete the cookie at any time through the options tab on your browser also outlined below. The cookie monitors your navigation through the website and records: 1) what content was viewed; 2) how you arrived at the specific content; 3) your ISP provider including the ISP providers geographic information; 4) the time spent viewing a specific piece of content; 5) the time spent on the entire website; 6) the path taken to access the website; and 7) the connection speed of the session. Google Analytics does not tell the Agency who you are or allow the Agency to determine your identity nor does the cookie monitor or record your web usage after you leave the Agency's website(s). The data is automatically sent from the cookie on your machine or device to Google's system which immediately aggregates the data. Neither the Agency nor Google will ever have access to the specifics of your particular session. What the Agency will see is the aggregate data from all users for a particular time period.

The Agency is gathering this information for internal purposes and has chosen to not share the aggregate data with Google. We may use the aggregated data to share with our partners and contractors to help improve the user experience. The Agency will retain the aggregated data as long as required per our records retention policy.

The Agency has taken great efforts to protect of users of the system.

2. What are the sources (people/systems) and types (categories) of the data/information in the system?

   FOIA requesters provide the information necessary to enable an agency to understand the records of interest and how to deliver the records requested. The agency in turn supplies correspondence and responsive records.
   Google Analytics provides the Agency with aggregate information depicting site usage activity.

3. Why is the information collected? (Purpose)

   To allow the public to submit and the agency to process FOIA requests and FOIA appeals. Collecting site usage activity is a common practice and the only means to determine how the public is actually using features on any given web site.

4. How is the information collected?

   Through a webform that is customizable by agency using the service.

5. Is this a paper and/or electronic collection of data?

   Electronically collected

6. How will the information be used by the Agency?

   To process FOIA requests and FOIA appeals.

   Google Analytic information will assist the Agency, its partners and contractors in identifying areas of the system to improve based on site usage.

7. If the system has been revised or terminated, are the original personally identifiable information (PII) elements still being collected or contained in the system? Yes_X__ No___. If no, what are the elements currently being collected? When did the collection of the original PII elements stop? How was the old data removed from the system?

   Yes

II. Access Controls for the Data

1. Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

   Yes—user roles are defined by level of privileges. All PII data collected on the system's webform are not available to public users.

2. Has the data in the system been encrypted according to the National Institute of Standards and Technology (NIST) requirements? **(Note: this requirement is for sensitive PII only)**

   Yes

3. Has the system undergone a risk analysis to identify harms that may result from technical failures, malevolent third parties or human error? Yes_X__ No___ (**Note: The risk analysis will help identify possible risks to the data in the system.**)

   Yes

4. How will you educate individuals/users having authorized access about the misuse of PII data? What type of training will users receive?

   Federal system users are provided with training that places emphasis on the protection of sensitive information and actions that can be performed within the system where potentially sensitive data can be released prior to their use of FOIAonline. Some agencies provide renewed training on an annual basis. Agencies are responsible for ensuring their users understand their obligation when accessing potentially sensitive information. Agencies using usernames and passwords to access the system are presented with "Rules of Behavior" which describe their responsibilities to protect and not misuse personal information contained in the system and are required to accept these conditions prior to gaining system access. All users are responsible for protecting the privacy rights of the requesters and appellants.

5. Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

   Individual contact information associated with a FOIA request is limited to the requester's name and organization which may be made available to public if the agency has made a determination to release it. Agency system users and support contractors have access to any additional requester information provided with the request. FOIAonline is supported by three separate contactor companies. These include CGI Federal for application development and support, Booz Allen Hamilton for managing the production environment, and Cherokee Services Group for tier I help

desk support. The above referenced FAR clauses are included in each of the contracts supporting the application.

Only the EPA and its agency partners and system management contractors have access to the aggregated information generated by Google Analytics.

6. Will other systems, agencies, state or local governments or other external parties (i.e., non-EPA) share or have access to information in this system? Yes_X__ No___. If yes, what type of agreement was issued *(i.e., ISA, MOU, etc.,)*? ***If any agreements were issued, please supply the Privacy Program a copy of the agreement.***

Yes, through memorandum of Agreements (MOA) with partner agencies. Copies of MOAs have been provided to the Privacy Program.

7. Will data and/or processes be converted from paper to electronic? If so, what controls are in place to protect the data from unauthorized access or use?

Data entered into the system either by the requester or agency user is in electronic form with access rights controlled by the user's role defined within the system.

III. Attributes of the Data

1. How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual.)*

All FOIA requests and appeals that are maintained within FOIAonline are assigned a tracking number based on submission time and date. (The first request of the FY is EPA-XX-2013-000001 and all requests are assigned subsequent numbers.) The system allows for registered users. A registered user can access a list of their requests by using a username and password they create. Responsive records, descriptions of requests, and requester names can be searched if the information has been made public by the receiving agency.

2. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the requested information? Yes___ No_X__ If yes, how is notice given to the individual? *(Privacy policies must clearly explain where the collection or sharing of certain information may be optional and provide users a mechanism to assert any preference to withhold information or prohibit secondary use.)*

No, requesters are required to provide a name and mailing address to make a FOIA request. FOIA requests do not include the presumption of privacy and are considered public requests. Requesters not willing to provide the required information through FOIAonline may submit their request through some other means to the agency (eg., mail), however agency processing requirements match the information required by FOIAonline to process a request.

3. Where is the privacy policy (paper-form)/notice (electronic-webpage) posted?

https://foiaonline.regulations.gov

4. Has a record control schedule been issued for the records in the system or the system itself? If so, provide the schedule number.

Yes, GRS-14.

5. While the data are retained in the system, what are the requirements for determining that the information collected remains sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

   FOIAonline is used to process FOIA requests and appeals. Records are maintained for a predetermined period of time based upon an approved, by the Archivist of the United States, record schedule (e.g., EPA maintains it records for a period of 2 or 6 years based upon GRS-14).

6. Will this system provide the capability to identify, locate, or monitor individuals? If yes, explain.

   No. A data monitoring tool has been installed to be able to track instances when an unusual amount of data have been access and downloaded as a means to detect potential cases of data misuse and to limit data breach events.

7. Does this system use any persistent tracking technologies?

   Yes. Google Analytics uses persistent tracking cookies to follow site usage activity, but this information on the specific user is masked by truncating their IP address and only aggregate information is stored and provided back to the Agency.

Must be approved by Administrator