United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: OGC Dashboard	**System Owner: Kraig Lattimore**
Preparer: Steven Wyman	**Office: Office of General Counsel**
Date: 08/13/2021	**Phone: 703-603-8882**
Reason for Submittal: New PIA_X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The Office of General Counsel (OGC) has an ongoing business process engineering and business process automation initiative which has helped the office reduce administrative labor costs while increasing employee effectiveness. Supporting this effort is a system of automated routines accessible through a "portal' interface called "OGC Dashboard." This system supports a series of automated routines, storing data in discrete databases which can then be queried to meet unique departmental business information needs.

OGC Dashboard serves OGC as a program application. Each of the OGC sub-offices inputs and maintains data specific to their missions. For example, the OGC office responsible for civil rights and environmental justice develops data pertinent to those subject areas; the office responsible for water legal matters maintains a separate data set in a different area of the app, and so on. Data present are used to inform staff and management, to prepare legal decisions, advice, and actions. The data in many cases become repositories to

help inform subsequent findings and management decisions.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

35 FR 15623 Stat. 2086

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

OGC Dashboard is developed in the Agency's Oracle ApEx platform. As such, it falls under the General System Security plan for that environment. It has been determined that OGC Dashboard will receive an Authority to Use (ATU) rather than an ATO. The ATU will be issued by OMS upon its completion of the ATU documentation review no later than quarter 1 FY 22.

1.3 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.

No ICR required. OGC Dashboard does not currently have a forms component, nor is one planned.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No. A cloud solution has not been determined, to date. When/if one is selected it will be a future version of the application. The data will reside on a dedicated OGC server within the National Computer Center.

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 system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

OGC Dashboard collects hundreds of data elements from different parts of the OGC program office ranging from case management and tracking, to administrative, legal notifications, reference citations, and more. Upon implementation of the system the data element dictionary will be shared with the System of Registries.

Certain segregable components of the OGC Dashboard contain the following PII data, which may be from applicants outside of EPA:

Summer Honors, Career Attorney Applications, and Honors Fellowships Applicants:
Name
Address
Email Address
School
Graduation Year
GPA
Veteran Status
Attached documents including resumes
Evaluator notes

Interdivisional Opportunities:
Applicant First Name
Applicant Last Name
Applicant Telephone Number

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

Data are collected from throughout the agency (eg. Program offices, regions) and input by OGC professional legal and administrative staff. Some data are program management, some pertain to legal case tracking. Each sub-program of OGC maintain their own data sets as determined by their business need.

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

No, there is no link to commercial data sources from OGC Dashboard.

2.4 Discuss how accuracy of the data is ensured.

It is the responsibility of OGC professional legal and administrative staff to ensure accurate data is placed in the application. A more formal data review has not been scheduled recently, but there is agreement within OGC offices that this will be done with the cutover from LotusNotes to Oracle ApEx.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is a low risk of unauthorized access, modification, deletion and/or release of sensitive data. The risk would common to nearly any electronic collection: An authorized user might mistakenly release information outside the system domain. To do this would be a violation of the OGC Dashboard Terms of Use.

Mitigation:

The Terms of Use are posted on the access page of the app and specify in the form of a user agreement that must be accepted that any form of CUI / PII in OGC Dashboard must be protected from unauthorized release.

OGC Dashboard is controlled through WAM authentication with additional access level administrative controls within the app. Data is compartmentalized by access controls and types of use. OGC Dashboard does not have non-OGC users, nor does it have an outward internet face/access. The app is maintained and used only by EPA OGC staff behind the Agency firewall.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 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, the OGC Dashboard does have access controls which control the categories of data to which individual users have access. The app supports all sub-offices of OGC and the first line of control (beyond password access to the application itself) comes from the segmentation of the datasets and then from role-based access within those datasets.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

A SysAdmin guide is being developed that specifies access controls to specific datasets.

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

As described under Section 3.1 above, the app supports all sub-offices of OGC and the first

line of control comes from the segmentation of the datasets and then from role-based access within those datasets.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Ongoing access to the OGC Dashboard is restricted to internal EPA OGC users. Development contractors as well as O&M contractors will have access to the data, as well.

Yes, the appropriate FAR clause is included in the contract which to date has been awarded to GDIT (General Dynamics) under GSA contract to EPA:

1. Task Order:
    a. GSQ0017AJ0037 of ITS EPA III

2. EPA Service Agreement (Account Number):
    a. DP39X0001 "WCF SUPPORT OF OGC"

Lotus Notes Migration

The required privacy language falls under the following sections of the GSA master contract:

1. https://www.acquisition.gov/far/52.224-1 "52.224-1 Privacy Act Notification"
2. https://www.acquisition.gov/far/52.224-2 "52.224-2 Privacy Act"

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Data are maintained for the life of the application. However, the types of data and use fall under EPA records schedule - EPA Records Control Schedule Number 1025. Information is destroyed after 10 years or after file closure, whichever occurs last.

Records need to be retained in anticipation of litigation, and the information life cycle must be maintained per the instructions in this schedule, and in accordance with Federal records use under the Title 36 Code of Federal Regulations.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

The data within OGC Dashboard are low risk. Some small amount of PII data does exist in the app but are protected according to role-based security protocols and system use and records management policies stated above in Sections 2.1, 2.5, and 3.5.

Privacy Risk:
There is a risk of keeping information longer than needed.

Mitigation:

The appropriate record controls schedule is followed.

Section 4.0 Information Sharing

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

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

There is no external sharing

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

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

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None: No external sharing

Mitigation:

None required

Section 5.0 Auditing and Accountability

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

5.1 How does the system ensure that the information is used as stated in

Section 6.1?

Access is limited to OGC attorneys, staff and contractors for the specific purpose. The system owner conducts new user training to ensure all users use information in accordance with the stated purpose. The system owner will also conduct user refresher training, as needed. The system owner also conducts quarterly system audits to ensure all users have the appropriate system access and are using their access to collect and review employment related information. Additionally, the system owner generates event logs to identify inappropriate or unusual activity, such as invalid login attempts, blocked login attempts, and failed login attempts.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

All individuals with access to the system undergo mandatory records management training, entitled "Records Management" through EPA's FedTalent learning management program, which includes how to handle SPII and PII in addition to annual Information Security and Privacy training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of improper/untimely audit

Mitigation:

The system owner also conducts quarterly system audits to ensure all users have the appropriate system access and are using their access to collect and review employment related information. Additionally, the system owner generates event logs to identify inappropriate or unusual activity, such as invalid login attempts, blocked login attempts, and failed login attempts.

Section 6.0 Uses of the Information

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

6.1 Describe how and why the system uses the information.

The OGC Dashboard developed organically within OGC from in-house expertise, originally in LotusNotes (LN). The Oracle ApEx version of the app is a combination of 18 LN databases onto a single Oracle database instance. We can refer to these subject areas as "components," and they are mostly segregable from one another, certainly so on the data layer. The sub-program offices of OGC directed the original development of the databases and are the providers and consumers of the data. OGC Dashboard is used to operate the OGC program and fulfill its mission.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_ No__X_. 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. Or any identifier that can be linked or is linkable to an individual.*)

Information is retrieved based on application categories as follows:

Summer Honors, Career Attorney Applications, and Honors Fellowships Applicants:

Name
Address
Email Address
School
Graduation Year
GPA
Veteran Status
Attached documents including resumes
Evaluator notes

Interdivisional Opportunities:

Applicant First Name
Applicant Last Name
Applicant Telephone Number

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

None.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Low risk of unauthorized use of information.

Mitigation:

The system owner also conducts quarterly system audits to ensure all users have the appropriate system access and are using their access to collect and review employment related information. Additionally, the system owner generates event logs to identify inappropriate or unusual activity, such as invalid login attempts, blocked login attempts,

and failed login attempts.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

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

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

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 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.

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

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

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: