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: Business Automation Platform - Salesforce** | |
| **Preparer: Timothy Hinds** | **Office: OMS** |
| **Date: 10/30/2020** | **Phone: 919-627-0670** |
| **Reason for Submittal: New PIA____ Revised PIA____ Annual Review__X__ Rescindment ____** | |
| **This system is in the following life cycle stage(s):** | |
| Definition ☐ Development/Acquisition ☐ Implementation ☐ | |
| Operation & Maintenance ☒ Rescindment/Decommissioned ☐<br><br>**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).**<br><br>**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 Business Automation Platform, the Agency's implementation of Salesforce Inc.'s Lighting Platform (a.k.a., "force.com") application Platform as a Service (aPaaS), is the Agency's strategic platform for business process automation. It provides database, workflow processing, user interface generation, declarative development, and other capabilities that are leveraged by applications consisting of configuration specifications that implement business logic. Several forms from the now-retired WebForms system were migrated into the Business Automation Platform (BAP), as have been various other applications from Lotus Notes/Domino. Additional applications have been and continue to be implemented on the platform.

No personal information such as DOB, SSN, nor any personal contact information such as address, telephone number, etc., is collected aside from Agency information that is publicly

available, such as employee name, Agency office telephone number, Agency office address, Agency employee ID, LAN ID, etc. This agency data, copied routinely by the ETL infrastructure into the BAP from the Privileged Account Status Tracking and Approval (PASTA) system, which has received it in turn from other Agency systems such as Active Directory, Oracle Internet Directory, the Federal Personnel Payroll System (FPPS, which is not PeoplePlus), etc., is stored in the platform as shared reference data.

Information in BAP is retrieved by applications.

# 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?

The BAP is not a system but rather an environment within which systems can be built. In the event that something is built that requires additional security than the BAP already has (such as an increased need for managing PII) that system will go through individual authorizations, just as any system would in another environment such as Java or C. Configuration of the BAP has been performed under authority of Section 8(a) of the Small Business Act (15 U.S.C. 637(a)), Federal Acquisition Regulation (FAR) Part 19.8, Contracting with the Small Business Administration "The 8(a) Program,", and General Services Administration Manual (GSAM) Part 519.870-4, Sole source requirements, in accordance with 41 U.S.C. 253(c)(5) and 15 U.S.C. 637(a).

## 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?

The BAP operates under Agency Authority to Operate (Expires September 30, 2021) at the FISMA Moderate level. The person-related data in the Platform comes from PASTA through the Agency's extraction, transformation, and load (ETL) infrastructure from other Agency systems, including Active Directory, Oracle Internet Directory, Locator, and FPPS, each of which has its own security plan and, where necessary, SORN. Individual applications operating on the platform are responsible for execution of their own Privacy Threshold Assessment, and, if warranted, Privacy Impact Analysis and SORN. The BAP is a secondary user of the data. The BAP does not reach out to the user to gather unique information that hasn't already been collected. The BAP centralizes information from the Active Directory (AD), PASTA, eIDW, and other resources in order to make it easier to find and locate an individual's information than is currently possible by having to go through multiple systems to find everything.

## 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 is required.

### 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?

Yes, Salesforce, on which the BAP is based, is FedRAMP certified. The Lighting Platform is PaaS.

## 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).

No personal information such as DOB, SSN, nor any personal contact information such as address, telephone number, etc., is collected aside from Agency information that is publicly available, such as employee name, Agency office telephone number, Agency office address, Agency employee ID, LAN ID, etc. This Agency data copied routinely by the ETL infrastructure into the BAP from PASTA, which has received it in turn from other Agency systems such as Active Directory, Oracle Internet Directory, FPPS, etc., is stored in the Platform as shared reference data.

A full identification of the shared reference data in the Platform is available in the BAP Application Deployment Guide (ADG). An excerpt of the ADG section addressing the Users and Contacts objects in the Platform is embedded here: The BAP is a secondary user of the information resources.

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

The information in the platform is copied from other Agency systems, including Active Directory, Oracle Internet Directory, FPPS, Locator, eIDW, and PASTA.

### 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.

### 2.4 Discuss how accuracy of the data is ensured.

Accuracy of the platform data is ensured at its Agency source systems. As data is updated in the source systems, the new data updates the BAP in the regular process of data migration through PASTA via ETL. In case of information change, the new data flows

from the source system to update the BAP on the standard cycle of download of data from that system.

### 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:**

No additional privacy risk is introduced by copying Agency data into the Platform. The ETL process of data load from PASTA to the BAP is automated.

**Mitigation:**

Privacy risk mitigation is a function of the source systems. In addition, the Business Automation Platform requires login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the BAP security plan.

## 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?

The BAP uses all the extensive access controls of the Salesforce Lightning Platform, including user and group profiles, permission sets, object-level permissions, record-level permissions, field-level permissions, and other fine-grained access controls. Detailed information is available at http://login.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf. The BAP enforces access control levels on data and functions available to any user according to the user's role, based on need to know. Access control levels include Administrator, Delegated Administrator, and application-specific levels. Each application in the BAP has a unique security profile restricting access to its data to those with a need to access it. The BAP enforces access restrictions by roles for each application, granting access to specific functionality and particular data as required by the application's design approved by the application owner.

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

Users authorized to use the platform for one or more applications have access to the shared reference data and data specifically restricted to the applications to which the user has been granted access. Access is determined through assignment of Salesforce Lightning Platform permission sets. The procedure for requesting access to an application through its permission set(s) is documented in the BAP User Provisioning Guide in the BAP Community Site.

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

No.

### 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?

Only EPA federal and contractor personnel with EPA network credentials, obtained through the Agency's standard process of network credential control and management, have access to the BAP. The BAP is a platform, such as SharePoint or the National Computer Center. Applications, each owned and managed by Application Owner, run on it. If an Application Owner grants access to the Application Owner's application to a contractor and FAR clauses need to be in their contract, the Application Owner is responsible for ensuring compliance. The platform administrator does not have insight into the status of FAR clause inclusion in the contracts of contractors among the application's user base.

### 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.

Information is retained as long as it is provided and not deleted by the source system. The BAP contains no Agency Records and has no EPA Records Control Schedule. The terms of use of the BAP include the agreement that the user not place Agency Records in the BAP, which is not an approved Agency Records Management System. Each application is different and should undergo a PTA, then possibly a PIA. If an application requires Agency-approved record-keeping, however, it is not suitable for the BAP, which is not an Agency-approved records management system. (We are working with the Enterprise Content Management System team to allow data from the BAP to be sent to ECMS, which is an Agency-approved Records Management System, for retention as records in accordance with applicable schedules, but the BAP will continue not to be itself a record-keeping system even once that interface is developed.)

### 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.*

**Privacy Risk:**

Low risk- applications hosted on the platform would keep data longer than needed.

**Mitigation:**

Applications will follow their corresponding record schedule.

## 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.

No**.** No data from the BAP is shared out to any system outside the Agency. The normal Agency operations in which data is accessed in the BAP are not performed by systems outside the Agency's network (including the network's remote access capability), nor do they result in transmission of data outside the Agency's network, including its remote access components.

### 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. Data is not shared externally.

**Mitigation:**

N/A

## 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?

The Business Automation Platform Program Office monitors the design, maintenance, administration, and use of the Platform for adherence to security and privacy standards. The BAP Program Office holds a Conceptual Review of each application as it is being architected and designed for use of the BAP, in which we review the application's data entities and relationships, user community, including roles and responsibilities, license requirements, etc. We review with

the application owner the use of shared objects and any restrictions on use of their data. The application owner must commit to adherence to any such restrictions and to passing those restrictions to the application and its users. The BAP PO next holds an Architectural Review of the application once it has been designed in detail, to assure that the application's structure and data is in accordance with the approved conceptual design, including any restrictions on data use. Finally, the BAP PO holds a Readiness Review to assure that the application has been tested and found in compliance with the approved design and all applicable data restrictions.

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

This is a function of the Agency source systems that collect the data.

This is an agency requirement to ensure all employees take the Security and Privacy Awareness Training.

### 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

**Privacy Risk:**

The risk exists that applications being hosted on the BAP could have inadequate privacy controls at the application level, not taking sufficient advantage of the controls provided by the platform. Auditing may expose risks. Application owners are accountable to mitigate risks.

**Mitigation:**

In conducting Conceptual Review, Design Review, and Production Readiness Review for an application, the BAP Program Office reinforces that the application must have sufficient privacy auditing and accountability controls in place. These reviews are described in section **Error! Reference source not found.**8.1.

## 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 Platform allows Agency personnel and applications to access the shared reference data for reference and integration purposes. The Platform does not, strictly speaking, use the information for any purpose other than to support applications built upon it The source systems provide data. Applications on the BAP using that data are different than source systems providing it. The source systems have various forms of documentation and agreements, including Memoranda of Understanding (MOU), Interconnection Security Agreements (ISA), ATO's, etc. Each application has documentation of its uses, including the use of data it accesses.

### 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.*)

The primary organization of the BAP is not by person, but by application.

### 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?

Each source system could have its own SORN, but as a secondary user of the information, no SORN is known to apply to the Platform.

### 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:**
No additional privacy risk is introduced by uploading Agency data into the Platform.

**Mitigation:**
Privacy risk mitigation is a function of both the source systems and the BAP security plan, which describes in detail the controls in place for the BAP. For example, the Business Automation Platform requires login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the BAP security plan.

***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:**