United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

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: OAP Salesforce	**System Owner: Alexandra Sullivan**
Preparer: Alexandra Sullivan	**Office: OAR-OAP-CPPD**
Date: 09/30/2021	**Phone: 202-343-9040**
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 ☐ **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 Atmospheric Programs offers a variety of voluntary programs to individuals and public and private organizations to promote energy efficiency, renewable energy, and greenhouse gas emissions mitigation. Many of these programs rely on Salesforce databases to communicate with partners and track program information. Specific programs with Salesforce platforms are:

(1) ENERGY STAR
The ENERGY STAR program is a voluntary government program that assists businesses and individuals in protecting the environment through superior energy efficiency.

ES Connect is the ENERGY STAR partnership/contact database system that resides on the Salesforce Service Cloud platform. It is comprised of basic ENERGY STAR partnership program organization information, program tools and reporting, and relevant business and partner contact

information. The information is utilized by EPA for the management of its voluntary relationship with partner organizations and communications with the associated partner contacts.

ES Connect is built on the Salesforce infrastructure which includes the Force.com platform. The Force.com platform is the foundation of the Salesforce application suite and provides security controls for the main ES Connect Lightning Service Cloud module and the My ENERGY STAR Account (MESA) Customer Communities instance within Salesforce. System components physically reside inside the government cloud of Salesforce U.S. data centers and are accessed by authorized users nationally/globally.

The main ES Connect Lightning Service Cloud and MESA modules include the following Salesforce capabilities and application modules:

Customer 360	Chatter
Leads	Salesforce 1 (Mobile)
Opportunities	Surveys
Case Management	Reports & Dashboards
Knowledge	Communities (MESA)
Data.com	

Within ES Connect, the Subscription Management System (SMS) utilizes Salesforce Marketing Cloud, a customer relationship management (CRM) platform and mass email service provider/platform. Marketing Cloud is integrated with ES Connect Service Cloud through the Marketing Cloud Connector App as an integral component that facilitates ENERGY STAR's program management of its partnership/participant marketing relationships and campaigns. Finally, ENERGY STAR leverages Case Management and Surveys within the Salesforce Lightning Service Cloud to support the ENERGY STAR Helpdesk and Portfolio Manager User Support Helpdesk.

(2) Green Power Partnership

The Green Power Partnership (GPP) program is a voluntary government program that assists businesses and organizations with increasing their voluntary green power use to advance the American market for green power and the development of those renewable electricity sources.

The GPP coordinates recruiting, account management, and outreach and communication activities with Salesforce (Sales Cloud licenses) in order to monitor, track store and communicate important program and partner information. The online CRM software serves as a database platform for program operations and as a digital repository and delivery system for program communications between EPA and its partner organizations. The GPP uses Salesforce to maintain partnership program information about its partners, their contacts, activity data, and recent and past communications. The GPP also uses Salesforce’s native communications platform to serve the core communications needs of the program. The native platform allows for seamless recording of outgoing communications executed through Salesforce and provides an ability to record incoming communications from Partners and stakeholders.

(3) Combined Heat and Power Partnership

The Combined Heat and Power (CHP) Partnership program is a voluntary government program that works with a network of CHP stakeholders to promote CHP’s role in providing affordable, reliable, and low emission energy.

The CHP Partnership coordinates Partner account management, outreach, and communication activities with Salesforce (Sales Cloud licenses) in order to monitor, track store and communicate important program and partner information. The online CRM software serves as a database platform for program operations and as a digital repository and delivery system for program communications between EPA and its partner organizations. The CHP Partnership uses Salesforce to maintain partnership program information about its partners, their contacts, activity data, and recent and past communications. Salesforce is the CHP Partnership's primary communication and Partner tracking tool. The CHP Partnership uses Salesforce in the following ways:

- Store Partner and CHP stakeholder organization and contact information. The Partner information in Salesforce is of current, former, and prospective Partners.
- Store records of communications with Partners and other stakeholders (including logs of helpline requests received and responded to).
- Track Partner CHP projects (although, as of a few years ago when the Partnership ceased Partner data collection, to a lesser degree).
- Maintain state and federal policies and incentives that appear in the online Database of CHP Policies and Incentives (dCHPP).

(4) Center for Corporate Climate Leadership

The Center for Corporate Climate Leadership (Center) is a resource center for all organizations looking to expand their work in the area of greenhouse gas (GHG) measurement and management.

The Center also uses Salesforce Sales Cloud licenses to maintain contact information on a range of corporate stakeholders to share program information and manage the Center's past awards program efforts.

(5) Non-CO_2 Programs Branch Voluntary Programs

The Non-CO_2 Programs Branch (NCPB) in OAP manages several industry partnership programs aimed at reducing emissions of non-CO_2 greenhouse gases (primarily methane). NCPB's programs (AgSTAR, Coalbed Methane Outreach Program [CMOP], the Global Methane Initiative, Landfill Methane Outreach Program [LMOP], Methane Challenge, and Natural Gas STAR) use a single instance of Salesforce (Sales Cloud licenses) to coordinate partner management, outreach, and communication activities so as to monitor, track, store, and communicate important program and partner information.

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 Clean Air Act Section 103(g). US Code 7403

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?

Yes, we have security plan ad ATO coverage under the OCSPP Salesforce ATO which was signed on 4/21/2020 and expires on 4/13/2023.

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.

Yes.
OMB Control Number: 2060-0528 (ENERGY STAR Partnership Agreements)
OMB Control Number: 2060-0347 (ENERGY STAR Commercial & Industrial Program)
OMB Control Number: 2060-0528 (ENERGY STAR Products Program)
OMB Control Number: 2060-0586 (ENERGY STAR Residential Program)
OMB Control Number: 2060-0578 (Green Power Partnership & CHP Partnership Programs)
OMB Control Number: 2060-0446 (Landfill Methane Outreach Program)
OMB Control Number: 2060-0722 (Methane Challenge Program)
OMB Control Number: 2060-0328 (Natural Gas STAR Program)

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, the data is stored in the Salesforce Government Cloud. Salesforce Lightning Service Cloud is FedRamp approved as a PaaS and SaaS. Marketing Cloud works with Salesforce Government Cloud but is not included in the authorization boundary of FedRamp. Marketing Cloud is captured under the EPA-OCSPP ATO that covers the operation of Salesforce. It is only used to send emails and communicate with customers and organizations, it does not store EPA data.

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).

(A) ENERGY STAR captures partnership program organization information, organizational relationship with the ENERGY STAR program, and relevant business and partner contact information. The information is utilized by EPA for the management of its voluntary relationship with partner organizations and communications with the associated partner contacts and other program participants. EPA uses Marketing Cloud to distribute emails to partners and other participants in the program. Organizations and consumers choose to receive these emails

voluntarily and can unsubscribe at any time. Specific pieces of information captured:

a. Limited PII (email addresses) for all email recipients
b. For Business participating in the ENERGY STAR Program as partners or otherwise:
    i. Organization name
    ii. Contact Name – salutation, first name, last name, suffix, nickname, and title
    iii. Business phone number
    iv. Business address –street, city, state/province, zip/postal code
    v. Role in the ENERGY STAR Program
    vi. Role in partner company
c. Individual consumers using ENERGY STAR tools and communications can optionally provide:
    i. Name - first name, last name

(B) Green Power Partnership captures partnership program organization information, organizational relationship with the program, and relevant business and partner contact information. The information is utilized by EPA for the management of its voluntary relationship with partner organizations and communications with the associated partner contacts and other program participants. The GPP uses Salesforce's native communications platform to distribute emails to partners and other participants in the program. Partners and stakeholders choose to receive these emails voluntarily and can unsubscribe at any time. Specific pieces of information captured:

a. Limited PII (email addresses) for all email recipients
b. For Business participating in the program as partners or otherwise:
    i. Organization name
    ii. Contact Name – salutation, first name, last name, suffix, nickname, and title
    iii. Business phone number
    iv. Business address –street, city, state/province, zip/postal code
    v. Relationship to the program
    vi. Role in partner organization

(C) Combined Heat and Power Partnership captures partnership program organization information, organizational relationship with the program, and relevant business and partner contact information. The information is utilized by EPA for the management of its voluntary relationship with partner organizations and communications with the associated partner contacts and other program participants. The CHP Partnership uses Salesforce's native communications platform to distribute emails to partners and other participants in the program. Partners and stakeholders choose to receive these emails voluntarily and can unsubscribe at any time. Specific pieces of information captured:

a. Limited PII (email addresses) for all email recipients
b. For Business participating in the program as partners or otherwise:
    i. Organization name

ii. Contact Name – salutation, first name, last name, suffix, nickname, and title
iii. Business phone number
iv. Business address –street, city, state/province, zip/postal code
v. Relationship to the program
vi. Role in partner organization

(D) Center for Corporate Climate Leadership captures stakeholder information, organizational relationship with the program, and relevant business and partner contact information. The information is utilized by EPA for the management of its voluntary relationship with stakeholders and communications with the associated contacts. The Center uses Salesforce's native communications platform to distribute emails to program stakeholders. Organizations choose to receive these emails voluntarily and can unsubscribe at any time. Specific pieces of information captured:
   a. Limited PII (email addresses) for all email recipients
   b. For Business participating in the program as partners or otherwise:
      i. Organization name
      ii. Contact Name – salutation, first name, last name, suffix, nickname, and title
      iii. Business phone number
      iv. Business address –street, city, state/province, zip/postal code
      v. Relationship to the program
      vi. Role in organization

(E) The Non-CO2 Programs (NCPB) capture partnership program organization information, organizational relationship with the program, and relevant business and partner contact information. The Programs also capture information on EPA activities (including site visits and workshops). The information is utilized by EPA for the management of its voluntary relationship with partner organizations, communications with the associated partner contacts and other program participants, and for tracking program accomplishments. Specific pieces of information captured:
   a. Limited PII (email addresses) for all email recipients
   b. For Business participating in the program as partners or otherwise:
      i. Organization name
      ii. Contact Name – salutation, first name, last name, suffix, nickname, and title
      iii. Business phone number
      iv. Business address –street, city, state/province, zip/postal code
      v. Relationship to the program
      vi. Role in partner organization

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

For ENERGY STAR, all information collected is provided voluntarily via a web form.

Green Power and CHP Partners must download a Partnership Agreement (PDF) from program websites, complete the document, print it, sign it, scan it and send it back to EPA, who then manually enters the data into Salesforce.

On the anniversary for each Green Power Partner, the program notifies each Partner that their annual reporting requirement is due. This includes exporting Partner data into an annual reporting form, which the Partner reviews, updates and sends back to EPA. EPA then manually enters any data updates into the Partner's Salesforce account.

The Center collects stakeholder contact information via email from organizations that choose the receive communications from the program.

The Non-CO_2 Programs collect all information voluntarily, either via Partnership Agreement Forms/Memoranda of Understanding (scanned PDFs), via direct emails to program managers, or via web forms. EPA then manually enters data into Salesforce.

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

Yes, we use commercially available location data for city, state, zip and country. This software provides regular updates to the database of city/zip combinations used to update the database for locations.

2.4 Discuss how accuracy of the data is ensured.

Basic data quality control checks are incorporated into Salesforce, for example to ensure zip code digit/length and valid domain and formatting for emails. The system also incorporates measures to compare records and prevent duplicate entry. Additionally, administrative modules allow authorized internal system users to review, correct, and or approve user/customer submitted data in accordance with established program SOPs and scheduled data quality checks and scripts.

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:

The primary risk to the characterization of the data is human error, which could result in the collection of inaccurate data. The information itself is categorized low risk because only limited PII is collected.

Mitigation:

As mitigation, the system avoids the collection of unnecessary data and does not capture any sensitive information. In addition, the data quality checks implemented in the system mitigate the risk of inaccurate data.

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. We give access to each system individually and provide limited access on an account level based on roles and privileges. Limited access to ES Connect Salesforce is available without authentication, an example of this would be a partner being able to submit a partnership agreement/sign up and provide certain information. Once this is established, external customers can access their own data only using password protected accounts that are powered by Salesforce Communities. EPA users have password protected access the Salesforce database.

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

Access to the Salesforce requires the purchase of a license and is only provided to EPA staff and contractors on an as-needed basis. EPA-approved Admin users can access regular user's information based on need (e.g. if the user is having a problem in their account or needs access to a module based on program management needs). Contractor development and maintenance staff, along with key EPA program managers are the only people who have Admin Access. This access is logged in the system – to enable tracking of any edits made by Admin Accounts. ENERGY STAR customers can only interface with the system via Salesforce Communities, with strict controls on the data that can be accessed and seen for each organization. The other OAP programs do not make use of this functionality.

These procedures are documented at the application level in concept of operation and system requirements documents located in the ENERGY STAR repository. The procedures for determining access to ENERGY STAR systems at the enterprise level are documented in the System Security Plan (SSP). Permission and security settings are stored within the Salesforce Security Settings Menu for the GPP, CHP Program, and the Center. Permissions configuration for the NCPB Salesforce system is documented in the NCPB Salesforce Administrator Documentation.

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

No other components are assigned within the system.

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?

Limited EPA staff and contractors have access to the data. The contractors that access our salesforce databases are covered by relevant clauses identified in the Agency's cyber security check-list and/or by the Rights in Data clause (FAR 52.227-14).

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.

Records where EPA has certified a result or provided official recognition, such as ENERGY STAR Awards or other similar records, are records that have operational value for the program but are not considered essential for the ongoing management of the program and therefore fall under EPA Records Schedule 1035, item c: Routine environmental program and project records. In the ENERGY STAR IT/IM system, users cannot delete this information (because it is saved by the program) and it is kept for at least as long as the record retention schedule of ten years.

Other records input by companies should fall under EPA Records Schedule 1035, item e: Other environmental program and project records. These records do not have value once they are superseded, updated, replaced, or no longer needed for the ongoing management of the program or project. This includes information input by users that are not certified by EPA. These files can be destroyed immediately after file closure. File closure, in this instance, includes when a company's information is updated, replaced, deleted by the company, and/or no longer needed for by current agency business. For more information, see here: http://intranet.epa.gov/records/schedule/final/1035.html

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. There is a risk that some records will be maintained longer than necessary.

Mitigation:

Data review and cleanup, including the removal of inactive records was performed as part of the migration from the legacy system to Salesforce. Going forward, the plan is to review data annually.

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. All data resides within EPA's borders.

As noted elsewhere, Salesforce hosts the database. Salesforce is authorized under an ATO led by OCSPP.

As discussed in Section 6, some (non-personal) information is published on the OAP Public Website in support of the program.

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

The purpose of the CPPD voluntary programs is to promote energy efficiency, renewable energy, CHP, and GHG management, and making information publicly available on energystar.gov and epa.gov is an inherent part of the program, as discussed in Section 6.

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?

OAP does not share information with any outside organizations and therefore does not have any MOUs or other special use arrangements with any outside parties as it pertains to OAP data.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable as there are no agreements.

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?

Not Applicable as there are no agreements.

Privacy Risk:

None. We don't share any information with outside parties, so there is no risk.

Mitigation:

None. We don't share any information with outside parties, so there is no risk.

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 information OAP collects is used to help public and private organizations and individual consumers find energy efficiency and clean energy products and solutions to protect human health and the environment. The primary control is access control. Only those EPA staff or contractors who need access to the information are provided with licenses and access to the systems for specific/intended EPA uses.

Separation of Duties and Role Based and Role Based Access Control is enforced to maintain access control. Custom profiles and permission sets have been established to control conditions for membership. Privileged functions with respect to Salesforce (modify

all rights, which are generally granted to the System Administrator) will be assigned only to the dedicated Sys Admin of the org. The general users will not have any over writing access

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

All privileged users receive annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk – risk of improper auditing.

Mitigation:

The primary mitigation strategies to ensure appropriate use of data are the implementation of access to specific users with a legitimate need to access the data for its intended purpose and the annual IT security awareness training to ensure users understand how to protect data confidentiality, integrity, and availability.

Most of the audit and accountability controls are inherited from Salesforce's Gov.Cloud. EPA's Salesforce instance allows system admins the capability to retrieve audit logs of all system events and user events for up to 6 months.

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.

OAP uses information to track participation in the programs (e.g. number of ENERGY STAR Products/Buildings/Plants, quantities of green power purchased, landfill gas projects, etc.) and to promote and expand the adoption of energy efficiency, renewable energy, CHP, and GHG management across the marketplace.

For ENERGY STAR ES Connect, a portion of the (non-private) partner information is made public (ENERGY STAR Partner organization names, website, city, state), on the ENERGY STAR website. ENERGY STAR qualified product information is also shared publicly on the ENERGY STAR website.

For the GPP and CHP Partnership, a portion of the partner information is made public on the respective program website and program communications (e.g., newsletters) in accordance with partnership agreements.

Contact information (email) is used to distribute communications to participating organizations, who may choose to unsubscribe from future mailings. Communications may be used to promote campaigns and share strategies for improve the performance of homes, buildings, and plants.

CPPD uses Case Management within Salesforce Service Cloud to communicate directly with partners and consumers via the Help Desk.

For the Non-CO_2 Programs, a portion of partner information is made public on the respective program websites in accordance with partnership agreements and memoranda of understanding.

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.*)

No. Information is retrieved by Organization Name.

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?

ES Connect access requires a Salesforce license authorized by the ES Connect administrator. The entry into the system for data access is via assigned username and password. The majority of information is contact information for businesses (not individuals), and the scope of information has been limited only to that data which is necessary. For example, if an individual signs up for a mailing list, they are only required to provide an email address and can unsubscribe at any time. Limiting the amount of data collected mitigates possible risk to people with information in the system.

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 –risk of an inappropriate use of data. .

Mitigation:

.Separation of Duties & role-based access control reduces the risk of data being used inappropriately. System admin users have the capability to review/retrieved audit logs and additionally check for suspicious activity. All users must be identified & authenticated before accessing any Salesforce components. The risk for unauthorized user activity is therefore low.

***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 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

<u>Mitigation</u>:

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 <u>Privacy Impact Analysis</u>: Related to Redress

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

<u>Privacy Risk</u>:

<u>Mitigation</u>: