Salesforce Enterprise PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: April 2022
(b) Name of system: Salesforce Enterprise
(c) System acronym: SF-DOS
(d) Bureau: Global Public Affairs (GPA/DIG/CRM)
(e) iMatrix Asset ID Number: 7455
(f) Child systems (if applicable) and iMatrix Asset ID Number:
(g) Reason for performing PIA:

☐ New system
☒ Significant modification to an existing system
☐ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

This PIA is being updated to add new data fields that are gathered in the system to assist with securing in-person events held for public outreach purposes. This information is not shared with external parties but is used to ensure registered guests and drivers for those guests are identified as those that registered.

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The Department of State uses Salesforce GovCloud Plus, known within the Department as Salesforce Enterprise, to serve as its centralized contact management database, which will enable staff to engage with members of the public domestically and abroad and maintain a robust history of those relationships. The Bureau of Global Public Affairs (GPA) manages the Salesforce platform both for its own offices and for other bureaus and offices in the Department, offering a shared service model resulting in greater efficiency than if each organization managed its own separate Salesforce instance.

Salesforce Enterprise provides the core contact relationship management module (CRM) and interrelated applications that capture personally identifiable information through contact records and a webform. Contact records are available to, but are not actively used by, all applications and functions in the GPA Salesforce environment. Custom applications are built on a cloud computing Platform-as-a-Service (PaaS) provided by Salesforce.

In addition to external contacts, the Salesforce Enterprise system contains a central repository of an employee's (user) profile data made accessible via a link on all the applications within the environment. Each Salesforce Enterprise user has an internal user profile, which provides them with the capability to log in to the system and use the basic functions such as Chatter messages (both shared and private) to one another to facilitate work collaboration. Chatter is an integrated social feature within Salesforce.

GPA's goal is to provide a global platform for contact relationship management, email marketing, event management, and related functions that is intuitive, accessible, secure, and bug-free, leveraging the built-in capabilities of the SaaS platform Salesforce.com, building custom code only when necessary to fulfill unique requirements. Salesforce is also a cloud-hosted environment running on Amazon Web Services that supports native functions as well as custom-built features that meet Department organizational needs.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Salesforce Enterprise Platform:

All users granted access to the Salesforce Enterprise platform are provided links to the Salesforce out of the box feature, Chatter. The Department of State's policy and guidelines restrict the information entered by Department staff about themselves (to include full-time employees and contractors) to the following elements of PII in the Chatter repository:

- Name
- Email Address (Government / business only)
- Telephone (Government / business only)
- Photo (Government / business only and optional)

Salesforce Enterprise contact information types:

PII and aggregate analytics will be collected and maintained in the Salesforce Enterprise environment throughout the lifecycle of the program. These data allow the Department to measure the effectiveness of its messaging to foreign and domestic audiences, build profiles about their audience members, and maintain ongoing relationships with contacts developed over years of outreach efforts. These applications collect two kinds of information about individual subscribers (*subscriber information* and *subscriber behavior*), but only subscriber information collects PII.

Subscriber information is information about specific subscribers; in all cases the individual explicitly opts in by entering information into the requested fields. An asterisk (*) identifies the only mandatory field for the core CRM module. New fields added since the December 2020 PIA was published are notated with the prefix *NEW:* below. Other fields may or may not be required for use in other Salesforce Enterprise applications or functions:

- *Name*: A combination of First Name (given name) and Last Name (family name)
- *Email Address*: The email address to use when sending out event invitations or mass email communications to this contact.
- *Mailing Address*: The business or personal postal address of the contact, comprising street address, city, country and postal code. Note that this mailing address does NOT go over to the email system. Only the country from a contact's address is passed over to the email system.
- *Title*: Any string, such as "Mr." or "Mrs." or "Herr" or "Madame"
- *Gender*: Male, Female or Unspecified
- *Phone number*: String value, as given and entered by the contact
- *Year of birth*: Year in which the contact is born.
- *Formal Name*: A concatenation of Title, First Name, Middle Name, Last Name. Can be overridden and replaced with any other text string by the CRM user. Sent to the email system for use in addressing the contact as part of invitations.
- *Email*: An alternative and/or additional email address to include office, personal, or other (may be the same or different from the preferred email address)
- *Phone*: An alternative phone number for reference by CRM module users which may include office, home, or mobile number.
- *Fax*: A fax number for reference by CRM module users.
- *Citizenship*: The country in which the contact indicated he or she has citizenship.
- *Web/Social Media:* The username of the contact in the following social media networks – Facebook, LinkedIn, Twitter, Instagram, YouTube, and other similar services in use locally.
- *Contacts*: The name of another contact who is the spouse, personal assistant, point of contact, or language translator of the contact. The spouse, assistant, POC and translator fields have email addresses which can be used as alternative email destinations for email invitations to the contact.
- *Biography*: A free-form description of the contact. Up to 32K characters long.
- *Dietary Restrictions:* A free-form field to identify any food preferences or allergies for event planning purposes.
- *NEW: Passport Number*: used optionally as a method to identify individuals invited to events at overseas posts, or as a method of identifying Diplomatic Reception Room tour participants at the Harry S Truman building.

- *NEW: Driver's license number*: used optionally as a method of identification for Diplomatic Reception Room tour participants at the Harry S Truman building, and for validating attendees at events at posts abroad.
- *NEW: Vehicle information*: Used to validate attendees at events at posts abroad, and can include Vehicle Number, Vehicle Color, Vehicle Make & Model.

Subscriber information is used by GPA, Regional Bureaus, and posts to tailor and personalize communications to a subscriber's expressed interests with content created by GPA or other bureaus with a presence in the Salesforce environment. Other fields inform event organizers about details for attendees that ensure each individual's preferences and position are handled appropriately during the event.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 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
- 5 U.S.C. 301, Management of Executive Agencies
- 22 U.S.C. 2651a, Organization of the Department of State

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Digital Outreach and Communications, State-79

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  January 27, 2016

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule numbers (e.g., (XX-587-XX-XXX)):

A-03-003-13, GRS 3.2 item 031 System Backups and Tape Library Records
A-03-003-04 GRS 3.1, item 020 IT Operations and Maintenance

- Disposition Authority Number:
  DAA-GRS-2013-0006-0004
  DAA-GRS-2013-0005-0004

- Length of time the information is retained in the system:
  A-03-003-13: Temporary; destroy six years after user account is terminated; longer retention is authorized if required for business use.
  A-03-003-04: Temporary; destroy three years after agreement, control measures, procedures, project, activity or transaction is obsolete, completed, terminated or superseded; longer retention is authorized if required for business use.

- Type of information retained in the system:

  SF Enterprise system backups such as contact records, event records, help desk case submissions, Chatter communications, and user account data which is maintained for potential system restoration in the event of a system failure or other potential loss of data.

  Operational and project records pertaining to system development, change management/system enhancements, policies and procedures, backlog of change requests, project performance, system performance, audit logs, administrator actions, and system security assessments.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

Salesforce Enterprise platform:

An administrator enters internal user's information into the system when an account is created using the information from an approved System Access Request Form (SARF, form number DS-4035).

Salesforce Enterprise's CRM module:

Data collected by the system (e.g., e-mail address, contact information, subscription preferences) are entered directly by the subscribers via a standard webform. This form always appears concurrently with a link to the Privacy Act statement governing the collection, either close in proximity to the webform or in the overall footer of the page. Subscribers may opt-out of the email list, or change their subscription preferences at any time, using a similar publicly accessible webform.

For basic contact management at posts, authorized staff may manually enter data or use input devices such as business card scanners to add contact details to the system. Contacts imported into Salesforce Enterprise from Department-supported legacy systems, e.g., eContact, Contact Management Database, Alumni Archive, have already previously provided consent for their email to be stored by and to receive communications from the Department on various topics. The import of this data maintains the opt-in status and retains consent to receive communications from the Department that the individual expressly previously gave on a per-topic basis, because the usage of their information has not changed.

Information about subscriber behavior, e.g., opening an email sent through the system, is collected in a manner consistent with industry best-practice via a small image file placed into the contents of email sent by the system. This image file is invisible to the user. The image file will only convey aggregate information about the subscriber accounts that opened the email and whether and when the interaction occurred.

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

Salesforce Enterprise is hosted on the Salesforce Government Cloud Plus (GCP) system, which has an agency sponsored FedRAMP authorization from the Department of Defense, Department of Energy, and Department of Health and Human Services that was reauthorized November 2, 2020. The platform is reauthorized every three years.

(f) What process is used to determine if the PII is accurate?

Data quality measures (i.e., data validation/normalization of data, PII is collected directly from individuals) are implemented at the initial collection or creation points and are repeated as the data are acted upon/utilized. These validation operations include functions like ensuring an email address is properly formatted or that a mailing address contains a valid country code. To the extent possible, data quality efforts are made to judiciously utilize data storage resources and ensure that only valid contact data are being stored in the system.

When an email is entered into the system, the system checks for the same email address across the database. If it finds one, it will prompt the staff member to likely update the existing record or affirmatively choose to create a new record (useful for families or schools who share email addresses).

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

A profile update link is included in all of the communication, which allows the subscriber to update their information. For those subscribers that have become inactive (e.g., an unread email, read email but no response), a follow up email is sent out at least annually, which includes a profile update link. Salesforce Enterprise also provides notifications on when emails were not successfully delivered, which often indicates that the email address used to sign up for updates is no longer valid; this can be used as an indication of when data have aged or become obsolete. In this case a subscriber will be removed from further subscription lists.

(h) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use commercial or publicly available information.

(i) How was the minimization of PII in the system considered?

GPA is concerned with the privacy of potential subscribers and has identified the minimum amount of PII needed to execute the mission and assess the effectiveness of the Department's communications. The system goal is not to build profiles of individuals, but rather to enhance the relationship with subscribers who desire to be actively engaged in the relationship. Thus, they voluntarily submit data as a part of this relationship.

This requires two types of information to be collected: *Contact* information that allows the Department to communicate with a subscriber electronically, and *demographic* information that allows the Department to tailor communications to subscribers.

With respect to demographic information, the system attempts to minimize the amount of information actually collected on an individual by only asking for the email address initially. By doing this and only asking for broad subscriber interests rather than specific demographic information the amount of PII collected is minimized. Posts are then able to tailor communications based on the subscriber's preferences over time.

5. Use of information

(a) What is/are the intended use(s) for the PII?

Salesforce Enterprise platform:

The internal user's information is used internally to provide appropriate access to the system, as well as to monitor resources and their allocation.

Salesforce Enterprise's CRM module:

The information collected is used to support the Department's public engagement mission by enabling posts worldwide and domestic offices to communicate with contacts through a modern, digital platform about topics relevant to their interests and USG policy goals. It also enables staff to perform protocol-related tasks to ensure that contacts are engaged appropriately. This factors in official titles and protocol, as well as the Department's history with a particular contact. The system also improves the USG's understanding of how best to communicate with audiences by providing message testing capability and aggregate email campaign analytics. These practices do not collect or generate any additional privacy-relevant information beyond that already outlined in this PIA.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, to be able to assess how well public outreach efforts help achieve Department or mission goals, Salesforce Enterprise users take advantage of the analysis tools that are built into the CRM module of the Salesforce platform. These tools provide a set of benchmarks used to monitor and evaluate the activity taking place in the aggregate, e.g., effectiveness of emails sent or responses to invitations.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the PII?
To evaluate platform adoption and how well contact management practices perform, benchmarks include audience email open rates and click rates, e.g., whether a recipient clicked on a link within the message, which are based on an assessment of average benchmarks for government agencies, and with consideration for other Department enterprise outreach efforts. Aggregated results are produced in consolidated reports and dashboards viewable by system users.

(2) Does the analysis result in new information?
Yes. It becomes possible to send more effective communications by selecting subsets of subscribers based on if they opened an email or RSVP'd to an event. It also helps offices determine if end users have adopted and are actively using the platform.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☒Yes ☐No

(d) If the system will use test data, will it include real PII?
☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:
In some cases, guest lists from events planned within the Events function in the CRM module may be exported and shared with Diplomatic Security domestically and Regional Security Officers (RSO) at missions overseas in order to undertake the Visitor Access Request process. The information will only be shared with Department employees and contractors in order to conduct the security review process (i.e., security guards, RSO staff).

External:
No PII is shared externally.

(b) What information will be shared?

Internal:
Guest information for mission or office-sponsored events would be shared, including guest names, sponsoring organization, guest headshot photo, and possibly seating assignment for seated events. For in-person events, vehicle information, e.g., make and model, color, license/tag number, and driver's license information, as provided in the registration form, would be shared.

External:
N/A

(c) What is the purpose for sharing the information?

Internal:
Information is shared so that Diplomatic Security and RSO can conduct security due diligence on event guests prior to in-person events. Vehicle and driver information is used by the Diplomatic Security (domestic) or Regional Security (overseas) staff assigned to in-person events to ensure that as guests arrive, that information can be validated against the registration form.

External:
N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
Salesforce enables credentialed users to export guest lists as Excel files or Word documents from Salesforce Enterprise. Those exported files would then be transmitted via Department email to appropriate DS and RSO staff.

External:
N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
The Salesforce Enterprise platform is accessed by specifically assigned profiles and roles; and each user is assigned a profile and role depending on the task assigned.

Internal users charged with facilitating the sharing of PII collected by Salesforce are expected to adhere to Department guidelines around the treatment of PII, including marking guest lists as SBU-PII and transmitting via Department email with appropriate markings.

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes. Webforms that enable a subscriber to sign up, unsubscribe, manage subscription preferences, etc. always appear concurrently with a link to the Privacy Act statement governing the collection, either close in proximity or in the overall footer of the page. Additionally, the double opt-in functionality also ensures that an individual is presented with privacy information a second time and takes an affirmative step to confirm they want to receive communications from the Department.

Contacts that may be imported into the system from existing lists maintained by posts from other systems have provided previous consent for their email to be stored by and to receive communications from the Department on various topics.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☒Yes ☐No

If yes, how do record subjects grant consent?

> When an individual uses the webform to subscribe to email communications, the system provides explicit notice during the opt-in process that explains to the individual what granting their consent will do and provides an unsubscribe option immediately if they do not wish to share the requested information. Further, an unsubscribe and preferences management capability is included in the footer of each email communication.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

For subscribers, an update preferences link and unsubscribe link are provided within the email notification they receive after subscribing or sending an email requesting information. This link allows them to see all of the information they've provided. In addition, when a subscriber initially subscribes to receive communications, they are given a link to update their subscription preferences – including opting out – at any time.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

For internal users, GPA provides redress via the Salesforce Support Helpdesk. An individual submits a request to the Helpdesk and once the update has been made a notification is sent to the user. If additional access or removal of access is required, an approved updated SARF is submitted with the required updates.

For external subscribers, an update profile link is provided in the email notification providing the option to update or correct their information at any time. The subscriber can update their information via the profile link at any time as long as they have the update profile link saved.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Internal users are informed via the initial confirmation email notifying them of their account that if any updates are required, they should contact the Helpdesk or submit an updated SARF (if it pertains to access).

For external subscribers, the initial and future email notifications provide an update profile link in the email footer for updating or correcting their information they submitted.

8. Security Controls

(a) How is all of the information in the system secured?

The Salesforce agency FedRAMP approved facilities are secured 24/7/365, which includes security guards at physical locations. Data systems are continuously monitored in accordance with industry best-practice and under FedRAMP guidelines.

Data is only stored in pre-identified data centers in the continental United States. Regular backups of the information are performed, which are encrypted and electronically stored. Technical controls (please see list below) are used to secure the FedRAMP approved servers that contain the information, which include but are not limited to:

- ID and Password protections
- Separation of duties and least-privilege access for system administrators
- HTTPS and Transit Layer Security (TLS)
- AES 128-bit Encryption of data at-rest, where necessary
- Firewalls
- Intrusion Detection Systems
- Multi-factor authentication

Periodically the security procedures are tested to ensure personnel and technical compliance per FedRAMP requirements.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

There are three primary types of system users: System Admins, Helpdesk/Configuration Users, and Internal Users.

System Admins and Helpdesk/Configuration Users: Have the ability to see all Salesforce Enterprise applications and PII system wide. Helpdesk/Configuration Users have a more limited set of permissions than System Admins, but they can implement a subset of changes to functionality and also troubleshoot any technical challenges a Internal User may encounter.

Internal Users: Can only access their applicable subset of data as required by their job function or their Mission assignment. They may either be assigned access to a specific Mission or Office's data or in some cases data for a particular region, depending on their assigned portfolio.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Internal access controls are assigned in a least-privilege manner to ensure that only personnel who have access to the information are those with a need to do so to perform their official duties. SARFs must be submitted and approved by the user's direct manager and system owner before an account is created.

(d) How is access to data in the system determined for each role identified above?

Access to the data is determined by assignable permissions based on a need to know in order to perform their job functions. These permissions are provisioned based on the submission of a SARF that is signed and approved by the internal user's supervisor (must be a Civil Servant or U.S. Direct Hire). In addition, technical restrictions are in place to ensure that Mission or Office staff can only see the data in their Mission or Office account.

System Admins: The Office of Contact Relationship Management (GPA/DIG/CRM) Office Director solely or in collaboration with the Program Manager, and Product and System Owner(s) assign individuals to the System Admin role. System Admins may be direct-hire or contract employees that have a background and skills managing IT systems, including the Salesforce platform, or may be trained to administer Salesforce Enterprise. System Admins manage access to SF-DOS for all other user types. They work with the IRM SE-ICAM team to ensure all users log into SF-DOS with the Okta identity management system. System Admins retain elevated privileges to perform administrative tasks until they change or vacate their job functions. They must have a Secret level clearance.

Helpdesk/Configuration Users: The Office of Contact Relationship Management (GPA/DIG/CRM) Office Director or Program Manager, together with the contract company program manager, determines who will perform in the Helpdesk/Configuration User role. The Help Desk/Configuration Users are all contract employees. They have full data and partial administrative access to SF-DOS, in order to perform specific duties required to resolve requests for assistance from users or to change configuration settings, perform data imports in coordination with bureaus as they add their contacts to the system. They typically do not have sufficient privileges to perform day-to-day administration of the Salesforce environment. These functions are limited to System Admins.

Internal Users: This is the default role assigned to the majority of SF-DOS users and is based on the information the individual enters into the SARF. At each overseas mission and domestic bureau, direct-hire managers select a number of internal users to be granted elevated privileges that allow them to perform functions not permitted for all other internal users. These actions include sending email campaigns, sending event invitations, merging duplicate contact records when they occur, and creating new entries to describe organizations that are associated with contacts. Internal users may view all of the contact data for their mission or office, but not others.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

Internal and external access safeguards (i.e., firewalls, intrusion detection devices, etc.) are employed to identify and prevent unauthorized access by outsiders that attempt to access the system, or cause harm to the information contained in the applications. The audit logs from these devices are automatically consolidated, summarized, and reviewed daily by the cloud service provider. Department access information is logged and audited periodically. Field history tracking is enabled for sensitive data items that may need to be tracked with a history of changes.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no role-specific training. Personnel are trained annually during the Department of State Cybersecurity training (Foreign Service Institute Course, PS800) on the privacy and security policies and compliance requirements. This training is required prior to providing access to the system and at least annually thereafter. Additionally, all OpenNet users are required to take the privacy course Protecting Personally Identifiable