PRIVACY IMPACT ASSESSMENT

Salesforce Enterprise

1. Contact Information

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

2. System Information

(a) Name of system: Salesforce Enterprise
(b) Bureau: Global Public Affairs (GPA/DIG/CRM)
(c) System acronym: N/A
(d) iMatrix Asset ID Number: 7455
(e) Reason for performing PIA:

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

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒ Yes
☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

Salesforce Enterprise (formerly IIP Cloud) received an Authority to Operate (ATO) for a Federal Information Security Modernization Act (FISMA) moderate rating in February, 2018. This PIA is being updated as part of the triennial ATO reauthorization for February 2021.

(c) Describe the purpose of the system:

The Department of State uses Salesforce GovCloud, known within the Department as Salesforce Enterprise, as its centralized contact management database. Salesforce Enterprise will enable staff to engage with members of the public domestically and overseas, while maintaining a robust history of those relationships. The Salesforce Enterprise platform contains three child applications: Contact Relationship Management (CRM), an internal helpdesk known as the Salesforce Support Desk, and a program tracking tool for public diplomacy known as PD Tools.

The CRM application captures personally identifiable information (PII) through contact records, while the other two applications are able to display the contact records stored in the CRM application. The multiple child applications are built on a cloud computing Platform-as-a-Service (PaaS) provided by Salesforce. The Salesforce Enterprise system provides a central repository of an employee's (user) profile data made accessible via a link on all the child applications. 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.

Beyond Chatter, the Salesforce Enterprise system provides a grouping of applications that supports programs managed by the U.S. Department of State's Bureau of Global Public Affairs.

Salesforce Enterprise includes the following applications:

Salesforce Enterprise CRM (SF-CRM)

SF-CRM is being used to provide a modern, mobile, unified application that captures contact information and historical data on Department external contacts and gives context to those relationships, while also offering a platform for robust email outreach and events management. SF-CRM meets the Department's need for better reporting and analytics, stronger communication among bureaus on contact outreach, along with scalable, flexible functionality that can adapt to changing needs.

GPA's goal is to provide a global platform for relationship management and email marketing that is intuitive, accessible, secure, and bug-free, leveraging the proven SaaS platform Salesforce.com.

Salesforce Support Desk

This application is used to manage email intake requests from Department of State staff, which are logged as cases/tickets for internal resolution. Capabilities included in the application are as follows:

- Service Console

- Automatic notifications to customers
- Email to case, converting email requests into support tickets
- Support processes
- Automated satisfaction surveys
- Manage ticket status, history and reports

The Support Desk does not process any PII. The contact records stored in the CRM Enterprise module are viewable in the Support Desk application so that Help Desk agents can see the basic contact information of the users (DOS personnel) who submitted the support cases. Agents can only see the contact records associated with submitted cases.

PD Tools

PD Tools is an application that offers Public Diplomacy practitioners an integrated set of audience analysis, strategic planning, management, and monitoring and evaluation tools. It leverages the SF-CRM application in its reporting and evaluation modules, eliminating the need for duplicate data entry.

PD Tools does not process any PII. The PD Tools application integrates with the events module in CRM, which allows users to tie embassy-managed events to the Mission's strategic plans. In this capacity, PII on event guests (through CRM guest lists) is visible to PD Tools users with the proper permissions, though all content is entered and processed through the CRM module.

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

All Applications:

All applications within the Salesforce Enterprise grouping provide 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)

SF-CRM:

PII and aggregate analytics will be collected and maintained in the SF-CRM throughout the lifecycle of the program. These data allow the Department to measure the effectiveness of its messaging to foreign audiences and build profiles about audience members. The application collects 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:

- *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 postal address of the contact, comprising street address, city, country and postal code. Note that this mailing address is not captured by 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*: This is a concatenation of title, first name, middle name, last name. The formal name can be overridden and replaced with any other text string by the CRM user. The formal name is 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 use reference by CRM users which may include office, home, or mobile number
- *Fax*: An alternative phone number for use reference by CRM users
- *Citizenship*: The country in which the contact indicated he or she has citizenship
- *Web/Social Media:* The username of the contact in social media networks – Facebook, LinkedIn, Twitter, Instagram, YouTube, and other. .
- *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 32,000 characters
- *Dietary Restrictions:* A free-form field to identify any food preferences or allergies for event planning purposes

Subscriber information beyond the mandatory field is used by GPA, Regional Bureaus, and posts to tailor and personalize communications to a subscriber's expressed interests with content created by GPA.

(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)?

☒ Yes, provide:

- SORN Name and Number: Digital Outreach and Communications, State-79
- SORN publication date: January 27, 2016

(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:

- Schedule number: A-37-008-07, GRS 3.2 item 040
- Length of time the information is retained in the system: Temporary; delete incremental backup files when superseded by a full backup or when no longer needed for system restoration, whichever is later.
- 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.

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 Lawfully Permanent Residences (LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐ Yes ☒ No (No SSNs collected)

(c) How is the information collected?

All Applications:

An administrator enters Department staff information into the system when an account is created using the information from an approved System Access Request Form (SARF).

SF-CRM:

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 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, staff may manually enter data or use input devices such as business card scanners to add contact details to the system.
When the system is first activated and when new posts are onboarded, a number of contacts may be imported into the system from existing lists maintained by posts from other systems, including the legacy systems eContact and the Contact Management Database. These contacts 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 DoS previously granted by the individual on a per-topic basis.

Information about subscriber behavior – email open rates, email click rates, browser used to open email, aggregate location of subscriber IP addresses, e.g. – is collected in a manner consistent with industry best-practice via a small image file placed into the contents of the email sent by the system. This image file is invisible to the user. The image file will only convey the aggregate information mentioned above about the subscriber accounts that opened the email and whether and when the interaction occurred.

(d) 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 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.

(e) What process is used to determine if the information 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 also 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).

(f) 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 communications, 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.

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

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

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes. Webforms that enable a subscriber to sign up, unsubscribe, manage subscription preferences, etc. appear concurrently with a link to the privacy 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 (when the system is first activated and when new posts are on boarded), have provided previous consent for their email to be stored by and to receive communications from DoS on various topics.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

Individuals may fully utilize GPA websites without subscribing to email communications.

Additionally, the system provides explicit notice during the opt-in process that explains to the individual what granting their consent will do and providing an unsubscribe option immediately. Further, an unsubscribe and preferences management capability is included in the footer of each email communication.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

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 USG to communicate with a subscriber electronically, and *demographic* information that allows the USG to tailor communications to subscribers. All information is collected voluntarily via double-opt-in, and collection forms are always displayed in close proximity to the relevant privacy policy. Moreover, every element of the collection is transferred from the signup box through the various systems involved via a secure HTTPS connection. This helps ensure the privacy and security of the personal data being transferred.

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 slowly over time.

5. Use of information

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

All Applications:

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

Salesforce Enterprise CRM:

The information collected is used to support the public diplomacy mission by enabling posts worldwide to communicate with engaged foreign audiences and U.S. citizens 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 foreign 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 information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

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

If yes:

(1) What types of methods are used to analyze the information?

The CRM Office uses benchmarking to monitor and evaluate the activity of the CRM Enterprise application, as well as the Salesforce Enterprise platform. The Office has predetermined appropriate benchmarks for successful platform adoption, and well as audience open rates, based on an assessment of average benchmarks for government agencies, and with consideration for other Department enterprise deployments. The 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 the office 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

6. Sharing of Information

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

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

No information is shared externally.

(b) What information will be shared?

Guest information for mission-sponsored events would be shared, including guest names, sponsoring organization, guest headshot photo, and possibly seating assignment for seated events.

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

Information is shared so that Diplomatic Security and RSO can conduct security due diligence on event guests prior to post-sponsored in-person events.

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

SF-CRM enables credentialed users at missions 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.

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

External sharing is disabled by DoS. Applications are accessed by specifically assigned profiles and roles; and each user is assigned a profile and role depending on the task assigned.

For internal sharing, employees 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. Salesforce Enterprise users are required to have OpenNet access, which requires annual completion of the Cybersecurity Awareness Course, which outlines Department policy on PII and SBU handling.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Guest lists shared with RSO and DS will contain PII, which introduces risk of data leakage. However, transmission should be limited to those who need to know this information for security purposes. To mitigate this, Department staff and contractors must handle guest lists in accordance to Department of State policy for handling and labeling PII, as outlined during annual Cybersecurity Awareness Training.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

For external 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.

(b) Are procedures in place to allow an individual 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 System Access Request Form (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.

(c) By what means are individuals 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 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 are 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 Secure Sockets Layer (SSL)
- 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) Describe the procedures established to limit 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.

(c) What monitoring, recording, and auditing safeguards 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. DOS access information is logged and audited periodically. And field history tracking is enabled for sensitive data items that may need to be tracked with a history of changes.

(d) Explain the privacy training provided to authorized users of the system.

Personnel are trained annually during the DoS 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 Information (PA318) every two years.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒ Yes ☐ No

If yes, please explain.

Technical controls are used to secure the information, but not limited to:

- Secure Socket Layer (SSL)
- Encryption
- Firewalls
- Intrusion Detection Systems
- ID and Password protections
- Multi-factor authentication
- Encryption at rest
- Encryption in transit

(f) How were the security measures above influenced by the type of information collected?

The Government FedRAMP compliant system (i.e. Salesforce Government Cloud) was chosen because personnel who handle or have access to the information must be American citizens with at least a secret security clearance. To be FedRAMP compliant a system must be authorized to operate at least as a moderate system. The Salesforce Government Cloud instance that GPA is using requires the security measures above as well as the personnel requirements (i.e. American citizen with a minimum of a secret security slearance) and is rated at FISMA Moderate.

9. Data Access

(a) Who has access to data in the system?

System Administrators, GPA Support staff, and System Users.

(b) How is access to data in the system determined?

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 System Access Form that is signed and approved by the requesting user's supervisor (must be a U.S. Direct Hire). In addition, technical restrictions are in place to ensure that Mission staff can only see the data in their Mission account.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Yes, this information is documented in the System Security Plan.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Data access is restricted by default and assigned in a least-privilege manner based on job function.

System Administrators and GPA Support staff have the ability to see all Salesforce Enterprise applications and data system wide, so they can implement functionality and also troubleshoot any technical challenges a system user may encounter.

System Users have access only to 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's data or in some cases data for a particular region, depending on their assigned portfolio.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

To prevent misuse, Salesforce Enterprise has put several controls into place. Controls fall into some key categories: Education and awareness, access controls, system monitoring, and platform encryption.

Anyone seeking access to the platform must have an active DoS OpenNet account, which requires annual completion of the Cybersecurity Awareness course (PS800) to ensure that users are well informed about methods to best protect data. In addition, system access requires technical training on the platform, which includes four days of classroom instruction on system use and best practices. End users must also fill out a SARF that explicitly outlines security policy and requirements for accessing the platform. By signing the access form, end users are agreeing to comply with the system policy. Finally, as part of the login process, end users will see a splash page that outlines the system's monitoring and data policy and states that logging in acknowledges consent of the system policy.

The platform has also implemented several access controls to ensure that data is only available to those who have a critical need. The SARF must be certified by a requestor's front line supervisor to validate that access is necessary and appropriate before an end user account is created. System permissions are set up to limit data to a specific Mission/Post, so that users only have access to the descrete data they require. Additionally, elevated permissions are only available to Protocol or Executive Office staff, as approved by a Executive office supervisor on the signed SARF. System Administrators, the most elevated users within the system, are required to have an active Secret Clearance, a SARF signed by the IT System Owner, and an official Salesforce (3rd party vendor) Administrator certification.

The Department has implemented Salesforce Shield, an advanced security package, to enable platform encryption, event monitoring, and audit logging to prevent data loss, leaks, and misuse. GPA's technical staff has applied encryption at rest to all PII fields in the SF-CRM applications. The platform also encrypts all data in transit, further protecting system data from intrusion. Event monitoring capabilities include dashboards and scheduled reports that display regular system activity and alert System Administrators of any suspicious activity. Monitored activity includes logins/logouts (including times and locations) and API calls. Event reports are run daily, and once a week the SF-CRM System Administrators will receive a reminder to review Event activity. Those activity logs are then audited by System Administrators and retained for six months for auditing and data retention purposes.