

**Email the completed PIA to  
[PIAteam@state.gov](mailto:PIAteam@state.gov)**

## **IIP Cloud PIA**

### **1. Contact Information**

**A/GIS/IPS Director**

Bureau of Administration

Global Information Services

Office of Information Programs and Services

### **2. System Information**

- (a) Name of system: IIP Cloud
- (b) Bureau: IIP/PL/DI
- (c) System acronym: IIPCloud
- (d) iMatrix Asset ID Number: 7455
- (e) Reason for performing PIA: Click here to enter text.
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

The primary purpose of this modification is to add the Public Diplomacy Customer Relationship Management (IIPCloud-PD-CRM) application. The IIPCloud-PD-CRM will provide posts with a modern, mobile-first contact management platform that will help build connections with foreign audiences that further public diplomacy policy goals. This unified system will provide posts worldwide with key functionalities; this includes: providing a mechanism to allow interested individuals—typically citizens of foreign countries—to subscribe to receive content from the U.S. government; sending e-mail messages to subscribers who have explicitly opted in to receive such communications; notifying subscribers of opportunities to engage more deeply with American public diplomacy by attending offline events like English language classes and cultural performances; and managing preferences such as those who wish to unsubscribe from future communications. The IIPCloud-PD-CRM, which is built on the Salesforce platform, includes an interface with Campaign Monitor, a mass-mailing application. Both Salesforce and Campaign Monitor are commercial cloud solutions hosted external to the State Department's computer network. In addition, since the last PIA (February 19, 2013), one child application (IIP Cloud Pitch System) has been decommissioned. Also, additional functions have been added, which include the System Access Request Form (SARF), Lessons Learned, and Content Management System (CMS) Risk.

### 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](mailto:IASolutionCenter@state.gov) for assistance.

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

Authority to Operate (ATO) documentation for the IIP Cloud platform for a FISMA Low rating is on-file as of July 31, 2013. Documentation to support processing FISMA Moderate rated data in the system for the PDCRM application is currently undergoing review within the normal agency triennial review process for adjustments to authorization in coordination with Information Assurance. The updated SCF was submitted in March 2016.

(c) Describe the purpose of the system:

The IIP Cloud system contains a group of multiple child applications with similar degrees of personally identifiable information and record subjects. The multiple child applications are built on a cloud computing Platform-as-a-Service (PaaS) and Software-as-a-service (SaaS) provided by Salesforce. The IIP Cloud instance of Salesforce applications provides a central repository of an employee's (user) profile data made accessible via a link on all the child applications. Each IIP Cloud 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. All users have the option to use Chatter, but there is no integration with any IIP Cloud child applications and the message records are fully managed.

Beyond Chatter, the IIP Cloud system provides a grouping of applications that supports programs managed by the U.S. Department of State's Bureau of International Information Programs (IIP).

IIP Cloud includes the following applications:

- **IIP Cloud Publishing Application (IIPCloud-PS)**

The Publishing application is the hub where content creators, editors and translators construct public-domain documents and articles in English and six other languages, and disseminate the documents to support the U.S. Department of State's public diplomacy efforts. The Publishing System disseminates this content by transmitting files to another Department system, IIP Digital.

- **IIP Cloud CO.NX Requests (IIPCloud-CO.NX)**

This child application offers a way to process interactive program requests from the field. It establishes a standard workflow and makes the request process accessible and transparent. Through the IIP Cloud CO.NX Requests application, the team will have a means of capturing program requests, moving requests through a workflow, and reporting on final outcomes from a desktop or mobile device.

- **IIP Cloud Project Management System (IIPCloud-PM System)**  
IIP Cloud Project Management System collects data on the contractor's tasks to include level of effort and time spent per task and deliverables, thus providing management with a robust reporting tool for the aggregation of information. It is an internal management reporting tool.
- **IIP Cloud American Spaces (IIPCloud-AS)**  
IIP Cloud American Spaces captures information on all categories of "Spaces" in the American Spaces Program to include facilities hosting American Corners, American Centers, Information Resource Centers, Science Corners, Binational Centers and Lincoln Centers.

IIP Cloud American Spaces will serve as a way to manually report on attendance at public events hosted at American Spaces worldwide. Aggregate counts only will be included in the system, with no information on individuals in attendance.

- **IIP Cloud PD CRM (IIPCloud-PD-CRM)**  
IIPCloud-PD-CRM will be used to provide a modern, mobile, unified application that captures contact information and historical data on IIP's and post's external contacts and gives context to those relationships, while also offering a platform for robust email outreach. IIPCloud-PD-CRM meets the Department's need for better reporting and analytics, stronger communication amongst bureaus on contact outreach, along with scalable, flexible functionality that will adapt to changing needs.

IIP'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.

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

**All Applications:**

All applications within the IIP Cloud grouping provide links to the Salesforce packaged application 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)

**IIP Cloud American Spaces:**

In addition to the Chatter profile link, the IIP Cloud American Spaces collects the following information about a person:

- Name (U.S. Department of State contact person for an “American Space”)
- Address, City, State/Province (Address for the “American Space” for which the person is the point-of-contact)

**IIP Cloud PD CRM:**

PII and aggregate analytics will be collected and maintained in the IIPCloud-PD-CRM throughout the life cycle of the program. These data allow the Department to measure the effectiveness of its messaging to foreign audiences and build profiles about their audience members. The application collects two kinds of information about individual subscribers (*subscriber information* and *subscriber behavior*):

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
- Email Address\*
- Mailing Address
- Title
- Gender
- Phone number
- Date of birth
- Topics of Interest

Subscriber information beyond the mandatory field is used by IIP and posts to tailor and personalize communications to a subscriber’s expressed interests with content created by IIP.

Subscriber behavior is information about how subscribers interact with communications sent through the IIPCloud-PD-CRM application:

- Email to an individual:
  - Date/time stamp of when an email was sent to a subscriber
  - Subscriber’s RSVP response status when invited via email to an event relating to their topics of interest
  - Email Opt-In status (true/false)

This capability only extends to email communications originating from the PD CRM; it does not track the subscriber’s browsing behavior in general.

In addition to these, the application collects and produces a number of aggregate analytics such as:

- Aggregate Active Subscribers by topic
- Aggregate Subscribers that are undeliverable by topic and the specific email sent
- Aggregate Unsubscribes by topic and email sent
- Aggregate Opened by topic and email sent
- Aggregate Not Opened by topic and email sent
- Aggregate Email Client Usage by email sent
- Event Management functions:
  - Aggregate RSVP acceptances
  - Aggregate RSVP declines
  - Aggregate RSVP not responded

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

- Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009.
- 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 (found under the Volume Number and above the Public Notice Number on the published SORN): 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 Division at [Privacy@state.gov](mailto: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](mailto:records@state.gov).)

If yes provide:

Chapter 37: Bureau of International Information Programs, Office of Web Engagement A-37-008-07 - Content Management System (CMS). Authorization Number: GRS 24, item 4a. Please note: IIP is working with Records Management to update the schedules to include the data in IIP Cloud.

#### 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:**

Department staff information is entered by an administrator when an account is created based on an approved System Access Request Form.

##### **IIP Cloud American Spaces:**

IIP Cloud American Spaces contact information is entered and maintained by an administrator.

##### **IIP Cloud PD CRM:**

Data collected by the system (e.g., e-mail address, contact information, subscription preferences) is 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; these contacts have already previously provided consent for their email to be stored by and to receive communications from IIP on various topics. The import of this data maintains the opt-in status upon import and retains consent to receive communications from IIP that the individual has expressly previously given on a per-topic basis, because the usage of their information has not changed.

Information about subscriber behavior – opening an email sent through the system, e.g. – 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.

(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.

IIP Cloud 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 effective May 23, 2014.

(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 is 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 is 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 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. IIP Cloud 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 has 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.

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

Yes. Webforms that enable a subscriber to signup, unsubscribe, manage subscription preferences, etc. always 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 IIP.

Regarding the 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 onboarded, these contacts have already previously provided consent for their email to be stored by and to receive communications from IIP 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 IIP websites without subscribing to email communications at all.

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?

The goal of the IIPCloud-PD-CRM application is to send communications to foreign audiences that are timely, relevant, and tailored to their interests. IIP is concerned with the privacy of potential subscribers and has identified the minimum amount of PII needed to execute this critical mission need and assess the effectiveness of the Department's communications. The usage of the system is not to build profiles of individuals, but rather to enhance the relationship with subscribers desiring to be actively engaged and voluntarily submitting data as a part of this relationship.

This requires collecting two types of information: *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. The strategy of asking for only the email address to get started, and then broad subscriber interests rather than specific demographic information helps minimize the amount of PII collected while enabling posts 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 for providing appropriate access to the system, resource monitoring and allocation.

### **IIP Cloud American Spaces:**

The American Spaces information is used to inform the public about the spaces, which in turn is used to support the Public Diplomacy efforts. The IIP Cloud American Spaces Database is a shared, scalable database that provides contact information, location, reporting and documentation for approximately 820 American Spaces worldwide. The Office of American Spaces (IIP/PL/AS) has the ability to create and edit American Spaces and IRO contact information, upload photos and files, sort and export information and run statistical reports on individual American Spaces entities.

### **IIP Cloud PD CRM:**

The information collected is used to support the public diplomacy mission by enabling posts worldwide to communicate with engaged foreign audiences through a modern, digital platform about topics relevant to their interests and USG policy goals. The usage of the system is not to build profiles, but rather to enhance the relationship with subscribers desiring to be actively engaged. 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?

A mixture of quantitative methods are used to monitor and evaluate the email communications activity and 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.

- (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.

### **All Applications:**

Staff information is shared with Department management.

### **IIP Cloud PD CRM:**

The information will only be shared with DOS employees and contractors (i.e., campaign managers, Program Officers, webmasters, Public and Cultural Affairs Officers, and support staff). Employees at individual posts will have access to post-level information; employees in Washington, DC and regionally will have access to information globally and regionally within the system.

- (b) What information will be shared?

### **All Applications:**

Access permissions are granted in a least-privilege manner (i.e., who is authorized to read/write/delete, etc.) And resource availability, contact information, and activity metrics are shared within posts and with management in order to make communication, budget, and resource management decisions.

**IIP Cloud PD CRM:**

Contact information, metrics, aggregate analytics and any communication sent or received are shared.

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

The information shared internally supports the internal auditing process and improving our products and services. It is used to build shared knowledge of communication practices across the various organizations engaged in public diplomacy, e.g. what types of communications work best for which audiences, or which regions seem to be most engaged on certain PD topics.

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

**IIP Cloud PD CRM:**

Within DOS, access to the information is controlled via IP-based authentication through OpenNet with a login and password required. Additionally, all users must utilize two-factor authentication for system access as an extra layer of security.

- (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.

Contacts data is accessed by role, region and country that are assigned to a user who owns/manages the contacts list. Access is provided based on the need to know principles of least-privilege, which dictates the permissions per user and are implemented as part of the access controls. System access requires a valid DOS OpenNet account and a Salesforce login and password, which is authenticated in the application at the time of access.

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

The ability to identify an individual by sharing several pieces of PII was a concern. The concern was addressed by keeping the amount of PII collected to a minimum and further by reducing the amount of data to be shared. This is also addressed at the frontend by providing a clear privacy policy to subscribers who opt in to providing information and at

the backend by ensuring the data is only transmitted within the system via HTTPS, providing extra security against unauthorized access.

## 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. 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.

- (g) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes  No

If yes, explain the procedures.

For internal users IIP provides redress via the Office of Digital 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.

Eventually the topics will be a “self-service” type of web page where contacts can control which lists they are part of in addition to being able to unsubscribe from any email we send them.

- (h) 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 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 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 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. Access requests (SARFs) must be submitted and approved by the user’s direct manager and system owner before an account is created.

(i) 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 too authorized users of the system.

Personnel are trained annually during the DoS Cybersecurity training (Foreign Service Institute Course, PS-800) 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. In addition, privacy training will be provided by IIP prior to the roll out of the system.

- (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

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

The requirement that personnel handling or having access to the information must be American citizens with a minimum of Secret Security Clearance, is the main reason for choosing the Government FedRAMP compliant system (i.e. Salesforce Government Cloud). To be FedRAMP compliant a system must be authorized to operate at least as a moderate system. The Salesforce Government Cloud instance that IIP is using requires the security measures above as well as the personnel requirements (i.e. American citizen with a minimum of a Secret Security Clearance) and is rated at FISMA Moderate.

## 9. Data Access

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

Privileged users/system administrators who have at least a need to know and have been approved by the System Owner and direct manager have access to the data. System users have access only to their applicable subset of data as required by their job function.

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

By assignable permissions based on a need to know in order to perform their job functions.

- (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.

- (j) 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.

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

Several controls are in place, including identification and authentication controls, banner reminders that activity on the system is monitored, need to know access restrictions, and reviews of audit logs.