Template Version Number: 01-2021

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Customer Interaction Platform - Salesforce (CIP-SF)

■ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.02.20 14:59:52 -05'00' 2/20/2025

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Customer Interaction Platform - Salesforce (CIP-SF)

Unique Project Identifier: EBPL-CCE-03-00

Introduction: System Description

Provide a brief description of the information system.

Customer Interaction Platform - Salesforce (CIP-SF) system provides a customer relationship management and event management service to the United States Patent and Trademark Office (USPTO) and its customers. CIP-SF primary focus is to manage and log customer inquiries, including all actions taken by the business units to resolve the service request. It can also create tickets to easily track requests.

Anyone can contact USPTO contact centers or Event Management Business Unit (BU) via telephone, email, or through mail/fax. Service requests will be automatically created by CIP-SF or if necessary, can be manually created by USPTO employees or contractors. The service request will include a summary of the telephone call and/or the content of any written communication, the contact information and a service request number. The USPTO employee or contractor that ingests the service request will route, if necessary, the service request to the appropriate BU for assistance. Once the service request is complete the service request will be closed. USPTO will generate pseudo-anonymized reports on data captured in the service requests. The Personally Identifiable Information (PII) within the system will be retained in accordance with the records control schedule, and if allowed per the record control schedule anyone contacting USPTO contact centers or Event Management BU may request their PII be deleted, the service request would then be pseudo-anonymized with only the service request number being saved and provided to the inquiring party.

- External customer contact USPTO contact centers or Event Management BU via phone, email, voicemail, Postal mail and event registration.
- CIP-SF end-user will create a service request to include the customer's contact information and reason for the service request (If user doesn't not want to provide contact information, then a service request will be created without contact information).
- End-user will service the customer or transfer to the appropriate BU for assistance (If user doesn't not want to provide contact information, then a service request will be created without contact information).
- If the customer is transferred from one BU to another, then the service request is also transferred with actions documented.
- Customers are provided a reference number associated with the service request.

- Service request is documented from initial contact to final resolution.
- For emails, a service request is created and the CIP-SF end-user replies to the customer's initial email.
- If an email is transferred, the CIP-SF end-user, update the service request and then forwards the service request and/or email to the appropriate contact center or BU for assistance and notifies the customer that the email has be forwarded.
- Reports are generated based on data captured in the service request and made available as requested.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

CIP-SF is a major application

(b) *System location*

CIP-SF is hosted on the Salesforce Amazon Web Service (AWS) Federal Risk and Authorization Management Program (FedRAMP) certified GovCloud system.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

CIP-SF is interconnected to:

Enterprise Contact Center (ECC) – provides Computer Telephony Integration (CTI), Automatic Call Distribution (ACD) and Interactive Voice Response (IVR) services to the USPTO and its customers.

Enterprise Office Software Services (EOSS) – provides Email Services. CIP-SFloud integrates with EOSS' Email as a Service (EaaS) infrastructure to send and receive email.

Identity as a Service (ICAM IDaaS) – provides unified access management across applications and API based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

Enterprise Data Warehouse (EDW) – provides access to integrated USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

Qualtrics XM (CXM) – display surveys and capture qualitative and quantitative user feedback from websites/applications.

Qradar – export Salesforce log files to Qradar through an Application Programming Interface (API) bridge.

Microsoft Office 365 (O365 MT) – a line of subscription services offered by Microsoft as part of the Microsoft Office product line.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Anyone can contact USPTO contact centers or Event Management Business Unit (BU) via telephone, email, or through mail/fax. Service requests will be automatically created by CIP-SF or if necessary, can be manually created by USPTO employees or contractors. The service requests may be manually created by USPTO employees or contractors for requests such as through telephone, email, or through mail/fax. The service request will include a summary of the telephone call and/or the content of any written communication, the contact information and a service request number. The USPTO employee or contractor that ingests the service request will route, if necessary, the service request to the appropriate BU for assistance. Once the service request is complete the service request will be closed. USPTO will generate pseudo-anonymized reports on data captured in the service requests. The PII within the system will be retained in accordance with the records control schedule, and if allowed per the record control schedule anyone contacting USPTO contact centers or Event Management BU may request their PII be deleted, the service request would then be pseudo-anonymized with only the service request number being saved and provided to the inquiring party.

- External customer contact USPTO contact centers or Event Management BU via phone, email, voicemail, Postal mail and event registration.
- CIP-SF end-user will create a service request to include the customer's contact information and reason for the service request (If user does not want to provide contact information, then a service request will be created without contact information).
- End-user will service the customer or transfer to the appropriate BU for assistance (If user does not want to provide contact information, then a service request will be created without contact information).
- If the customer is transferred from one BU to another, then the service request is also transferred with actions documented.
- Customers are provided a reference number associated with the service request.
- Service request is documented from initial contact to final resolution.

- For emails, a service request is created and the CIP-SF end-user replies to the customer's initial email.
- If an email is transferred, the CIP-SF end-user, update the service request and then forwards the service request and/or email to the appropriate contact center or BU for assistance and notifies the customer that the email has be forwarded.
- Reports are generated based on data captured in the service request and made available as requested.

(e) How information in the system is retrieved by the user

USPTO employees and contractors can retrieve information in the system by logging into the web-based interface through ICAM-IDaaS. Users are logged in using authorized user's role-based access control. The user can run a general search query to pull up the service request that they have access to, pulling the customer contact information, or to run ad hoc reports.

(f) How information is transmitted to and from the system

Information is automatically transmitted to and from the system via user input via email and event registration. For postal mail, fax, and phone calls the service request is manually created by USPTO employee or contractor. Information is directly ingested by CIP-SF automatically creating a service number or in some situations manually entered by USPTO employees or contractors. Customers will be notified by the system if their service request is assigned to another USPTO employee or contractor and when the service request is closed or if USPTO employees or contractors responds to their request.

(g) Any information sharing

There are no interconnections to share information outside the agency.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

35 U.S.C. 2, Powers and duties
5 U.S.C. 301, Management of Executive Agencies
Executive Order 12862, Setting Customer Service Standards

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☒ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify): Service Request Number Department of Corrections Inmate number for publication fulfillment request *No longer provide the service* However the inmate number is captured to send a letter informing the inmate that we no longer offer the publication fulfillment service.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☐

b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☒	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify): Mailing address					

Work-Related Data (WRD)					
a. Occupation	☐	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☐	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☒	g. Work History	☐	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify): Attorney information or law firm information. Business Type– Minority Owned or Veteran Owned					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	f. Scars, Marks, Tattoos	☐	k. Signatures	☐
b. Palm Prints	☐	g. Hair Color	☐	l. Vascular Scans	☐
c. Voice/Audio Recording	☒	h. Eye Color	☐	m. DNA Sample or Profile	☐
d. Video Recording	☐	i. Height	☐	n. Retina/Iris Scans	☐
e. Photographs	☐	j. Weight	☐	o. Dental Profile	☐
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☒	f. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify)
Any other PII an individual chooses to provide

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☒	Hard Copy: Mail/Fax	☒	Online	☒

Telephone	☒	Email	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data quality checks are integrated into CIP-SF. These are integrated at the initial collection or creation points and are repeated as the data is acted upon/utilized. These quality check operations include functions that ensure the quality of the contact information, for example ensuring an email address is properly formatted or that mailing address contains a valid country code. When an e-mail is entered into CIP-SF, the system will check for the same contact information across the database. If it finds a match, it will prompt the USPTO employee or contractor to choose between updating the existing record or choose to create a new record.

CIP-SF collect information directly from the individual, allowing them to provide accurate information while providing notice of collecting PII at the time of collection, minimizing the risk of inaccurate data collection. To mitigate these risks the USPTO implemented controls that restrict access to data and changing permissions to restrict changes to information by unauthorized parties, regularly backs up data that can be restored in the event of an unauthorized modification of data, and maintains audit logs to determine when data is added, modified, or deleted.

The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0080 Generic Clearance 0651-0078 Ombudsman Survey 0651-0057 Patents External Quality Survey

☐	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify): Emails received and postal mail, in-person.			

☐	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☒	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☐	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☒

For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The contact information in CIP-SF is for customers contacting the USPTO. Customers can be anyone. In the event an individual is requesting information and is currently housed in the Department of Corrections their Department of Corrections Inmate number will be required for USPTO to provide a response. CIP-SF is a technology for managing relationships and interactions with customers. It helps USPTO stay connected to customers, streamline processes, and improve the customer experience. CIP-SF can be used to enable USPTO employees and contractors to appropriately respond to customers.

USPTO employees and contractor's work information is used internally to provide appropriate access to the system and to monitor the resource and allocation. This is not in relation to the generic clearance mentioned in section 2.3.

Event Management – Gender and Date of Birth (DOB) information is used in CIP-SF to book travel for registered attendees.

Entity Type – Only use to aggregate data on a case-by-case bases via Data Call

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be

immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information. The USPTO requires annual training for system users regarding appropriate handling of information, automatic purging of information. NIST security and privacy controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☒	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify): The individual with whom the service request pertains. The Gender and Date of Birth (DOB) of registered attendees of USPTO events are used for booking travel.	☒	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ICAM-IDaaS EOSS ECC EDW Qualtrics XM NIST security and privacy controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: Customers are notified while in the phone menu before they are connected to an agent for service. "You may be asked to provide identifying information that will be collected and used by the USPTO Contact Centers/Event Management to facilitate customer assistance. Furnishing this

		information is strictly voluntary. More information is available at https://www.uspto.gov/privacy-policy".
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Customer may specify that they do not want to provide information. If the customer declines to provide contact info or PII, then a service request is created without the contact information/PII. Event Management registrants are required to provide First and Last Name, Zip Code and Email Address. Speakers are also required to give First and Last Name, Zip Code, Email Address, and Phone Number.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: *USPTO Employees

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The PII/BII used in CIP-SF is collected only to answer the queries from the customer the customer can request that the PII/BII be pseudo-anonymized upon the closure of the ticket but does not have the opportunity to consent to particular uses of the PII/BII.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: PII/BII cannot be updated directly in CIP-SF by the customer, however the customer can call USPTO customer service center to request to review and/or request updates to their PII/BII that was previously given.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: audit trails.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 5/29/2024 ☒ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☐	Contracts with customers establish DOC ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/PAT-TM-20 Customer Call Center, Assistance and Satisfaction Survey Records.
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: DAA-GRS-2017-0002-0001 Item 010 - General Records Schedule 6.5: Public Customer Records DAA-GRS- 2013-0005-0004 -Item 020 - Information Technology Operations and Maintenance Records
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☐
Degaussing	☐	Deleting	☒
Other (specify): Follow records retention schedule with Records Archive			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

☐	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Customer's name, email, address, and phone number to create a record can be used to identify an individual.
☒	Quantity of PII	Provide explanation: Approximately 500,000 per year
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements and does not include sensitive identifiable information.
☒	Context of Use	Provide explanation: CIP-SF collects the customer information to create a service request. It documents, supports, request to provide service or register customers for USPTO events. To capture and track the customer's interactions. Collect the public customer information that call into USPTO.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: Access to the PII is limited to USPTO employees and contractors that require the information to perform their official duties. The PII is securely stored in the Salesforce AWS FedRAMP certified Government Cloud.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the

choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to cloud data centers servers is restricted to authorized personnel. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO/Cloud providers monitor, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.