Template Version Number: 01-2020

U.S. Department of Commerce
International Trade Administration (ITA)

Privacy Impact Assessment
for the
ITA Salesforce Platform

(ITA-SFPF)

Reviewed by: Timothy Chad Root, Bureau Chief Privacy Officer

[X] Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
[ ] Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 05/19/2021

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

U.S. Department of Commerce Privacy Impact Assessment
International Trade Administration / Salesforce Platform
(ITA-SFPF)

Unique Project Identifier: 2520

Introduction: System Description

Salesforce Platform (SFPF) is a FedRAMP certified application that helps facilitate the International Trade Administration's (ITA) mission by enabling collaboration and information sharing. The Salesforce information system includes the Force.com platform, applications built on top of the platform, including SFPF and the supporting Salesforce infrastructure. The Force.com platform is the foundation of the Salesforce.com application suite and provides security controls for the SFPF instance within Salesforce. The Force.com platform is a Platform-as-a-Service (PaaS) in a public multitenant cloud model, enabling developers to create and deliver any kind of business application entirely on-demand and without software. The platform includes easy-to-use, point-and-click customization tools to help customers create solutions for unique business requirements, without any programming experience. Salesforce.com has developed custom applications that is built on top of the Force.com platform and relies on the platform for security controls. The Salesforce applications extends the platform capabilities to offer Salesforce.com developed and delivered enterprise applications like customer relationship management and web applications. The web applications Salesforce is also integrated with Pay.gov and Elastic Search. ITA Sales Force Platform consistent of ITA-CRM, Web Application (such as www.export.gov, www.stopfakes.gov, www.selectusa.gov, www.privacyshield.gov and beta.trade.gov), Privacyshield App, Toolkits App, Qualtrics Survey System, ADCVD Case Management System etc.)

Customer Relations Management (CRM)

- The CRM App is a Customer Relations Management App that is used to manage relations between ITA, and the Organizations and Individuals interested in working with the ITA. This is an internal application, accessible only to ITA employees, who collect the information from external perspective clients through In-Person contact, Phone or email. Individuals can contact the ITA to provide, access, update or amend their information. CRM is used to monitor the system's performance, provide customer information to Federal agency and bureau partners, and Federal partners' sponsored organizations to further serve the customer, and to obtain customer feedback concerning their service experience and the level of satisfaction provided by SFCRM and the servingagency.

  Types of Personally Identifiable Information (PII) collected: Name, Title, Work Phone, Mobile Phone, Fax, Email, Address, City, State, Country, Zip Code, County (Auto

populates by 9-digit ZIP), and Congressional District (Auto populates by 9-digit ZIP). **None is publicly available.**

Internal: All PII and BII information are searchable and retrievable internally to authorized ITA employees with the need-to-know.

External: No PII and BII information fields are searchable or retrievable externally.

Web App

Web App is a Content Management System, which is built in Salesforce for publicly accessible International Trade Administration Websites (listed below), where ITA webmasters can manage/edit the content and these sites are hosting in Salesforce (force.com) Platform.

www.export.gov
www.privacyshield.gov
www.selectusa.gov
www.stopfakes.gov
beta.trade.gov

No PII/BII is collected. All information is for public consumption.

Knowledge App

Knowledge App is International Trade Administration's comprehensive Knowledge Base (KB) built in Salesforce, which is accessible internally (controlled by Permissions and Groups) as well as externally (through public websites). Here is the list of Knowledge base that is accessible publicly (delivered through websites like Export.gov, Privacyshield.gov, stopfakes.gov and selectusa.gov).

- Country Commercial Guide
- Basic guide to Exporting
- FAQs
- Market Intelligence
- Top Markets
- State Reports and
- Trade Agreements

No PII is collected. All information is for public consumption.

Privacyshield / Participation App

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

The Privacy Shield App is administered by ITA / U.S. Department of Commerce and enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from determinations whether data are secured to an adequate level of acceptance. To join either Privacy Shield Framework, a U.S.-based organization is required to self-certify to this App (accessible via Privacyshield.gov website) and publicly commit to comply with the Framework's requirements. The self-certified companies will be reviewed by the Privacyshield team and displayed in the website https://www.privacyshield.gov/list.

Information in Privacy Shield is collected through Online forms by/after registration and the individuals can login to their community and update their PII/BII information.

- **Types of PII collected:** Name, Email, Country, Postal Code, Address, Street, City, State, Postal Code, Country, Phone, Fax, and Title. **All publicly available, via PrivacyShield.govwebsite.**
- **Internal:** All PII and BII information fields are searchable and retrievable internally to authorized ITA employees with the need-to-know.
- **External:** No PII fields are searchable externally. However, the PII is available through Privacyshield List URL - https://www.privacyshield.gov/list, and BII information is searchable through Privacyshield List URL - https://www.privacyshield.gov/list.

Toolkits App

Toolkits will allow U.S. Exporters to learn about the global challenges, including those related to standards and regulations, facing select U.S. industries from the latest ITA Top Markets Report for the sector. The toolkits also include contact information for ITA industry analysts who are knowledgeable about global conditions in their sector of expertise.

Types of PII collected: Name, Email, Country, Postal Code, Address, Street, City, State, Postal Code, Country, Phone, Fax, Title. **None is publicly available.**

Internal: All PII and BII information are searchable and retrievable internally to authorized ITA employees with the need-to-know.

External: No PII fields are searchable externally. BII Information such as '**Organization Name**' and '**Solutions Provided**' are available through:

- Environmental Solutions Toolkits - https://www.export.gov/et_search
- Oil and Gas Toolkits - https://www.export.gov/og_search
- Renewable Energy Toolkits - https://www.export.gov/re_search
- NextGen Toolkits - https://www.export.gov/ng_search
- SmartGrid Toolkits - https://www.export.gov/sg_search
- Civil Nuclear Toolkits - https://www.export.gov/cn_search

AD/CVD

The Antidumping Duty and Countervailing Duty (AD/CVD) Case Management System is an internal application built on the Salesforce Platform. This application consists of data modeling, date calculations/automation, staffing and reporting/dashboards. Enforcement and Compliance (E&C) users currently engage with system by creating and staffing cases, inputting dates/Federal Register information and reviewing dashboards/reports, in order to successfully make it through their business process before a deadline passes. Only available to ITA Employees with the need-to-know.

No PII is collected.

Qualtrics is a Survey System we integrated with Salesforce to send out surveys to Contacts (External Client) upon Closing following types of Case in CRM App:

- Export Promotion
- Commercial Diplomacy
- Investment Promotion

Once the Case Owner (ITA Employee) Closes one of the Cases – Salesforce will trigger an **Outbound message** to **Qualtrics** to send out the survey to the **Case Contact** (External Client).

Survey Questions has been mapped with Salesforce fields:

Survey Number - Autonumber
Case Owner - ITA Employee

Primary Contact - ITA Employee
Contact - External Client
Case - Related Salesforce Case Number
Record Type - Type of Survey
Likely to Recommend - Survey Question
Objectives Met - Survey Question
Type of Information - Survey Question
Better Serve - Survey Question
Best Working with Us - Survey Question

The purpose of this system is to assemble the necessary information to assist customers in connecting with business assistance services, programs, data and other resources in a larger effort to help the economy by supporting small and medium sized businesses and exporters financial growth; as well as creating jobs that will help ITA in promulgating its mission by promoting and fostering international trade opportunities between small and medium sized U.S. business and international trading partners. This system serves as a controlled repository for customer data and available business resource summary information. The information obtained from the Salesforce

Salesforce.com has developed custom applications that is built on top of the Force.com platform and relies on the platform for security controls. The Salesforce applications extends the platform capabilities to offer Salesforce.com developed and delivered enterprise applications like customer relationship management and web applications.

The privacy notice can be found here:

https://www.trade.gov/privacy-program

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

(b) System location
Salesforce GovCloud (na21) – FedRAMP Approved

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Salesforce is a Standalone GovCloud system integrated with the following Systems/Applications (due to business needs):

- **Pay.gov**: Pay.gov is a secured government payment processing method used to collect the payments on behalf of Government Agencies. Pay.gov does not save credit card details or Automated Clearing House (ACH) information. ITA uses Pay.gov as their payment processing method and has been implemented for Salesforce Applications such as Privacyshield, where the application sits in Salesforce and securely directs to Pay.gov for the payment. Once the payment process is successfully completed by the user (in Pay.gov), it securely directs back to the Salesforce Privacyshield Application with a confirmation ID and status of the payment. ITA will collect the money directly from Pay.gov. **No PII is exchanged between Pay.gov and Salesforce.**

- **Elastic Search (EDSP):** ITA Salesforce is integrated with EDSP (Elastic Search). 1) Search functionality for the websites hosting in Salesforce, where EDSP/Elastic Search is pulling information and displays through Salesforce Websites such as https://www.export.gov/, https://www.stopfakes.gov/, https://www.privacyshield.gov/, https://www.selectusa.gov/ and https://beta.trade.gov/. 2) Search functionality for the sub-applications that sits in Salesforce hosted Websites like FTA (https://beta.trade.gov/fta), Global Steel Trade Monitor (https://beta.trade.gov/gstm) and CSL Search (https://export.gov/csl-search) and data sits in ITA AWS Server, in which Salesforce acts as an User Interface and connected with EDSP / Elastic Search as a Connected App, a Salesforce feature to integrate with external application using standard SAML and OAuth protocols to authenticate and provide tokens for use with Salesforce APIs.
  No PII is collected, and all information is available for public consumption.

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

For administrative matters
To improve Federal services online
To promote information sharing initiatives
For web measurement and customization technologies (single-session / multi-session)

ITA Salesforce sits in Salesforce GovCloud, which stores Data and Metadata in two of Salesforce's U.S. collocated data centers with one acting as the Production site and other as the fully redundant disaster recovery Site. Security controls are consistent between data center locations.

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

ITA Users and Community Users can access the system through any browser with internet connectivity (and proper authentication). Websites hosting in Salesforce are publicly accessible through a browser. Individuals can contact ITA to provide, access, amend or update their information. No information can be retrieved by a unique identifier.

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

Most of the data transaction between the User and system is through Online browser.

CRM, an internal application, is accessible only to ITA employees who collect the information from external clients through In-Person contact, Phone, or email. Individuals can contact the ITA to provide, access, update or amend their information. Connection to pay.gov is a result of a user being forwarded to their page external from Salesforce and its applications. Pay.gov is not a part of Salesforce.

(g) Any information sharing conducted by the system

CRM

ITA is sharing the following information of Successfully Closed Export Promotion (with the exception of No Fee-Based Services Used) CRM Cases with EXIM Bank.
Contact (External), Contact Email (External), Case Owner (ITA employee), Organization / Account Name, Organization / Account City, Organization / Account Country, Organization / Account County, Organization / Account State, Organization / Account Street, Case Number, Case Status, Case Type, Subject, Fee-Based Services
ITA-Salesforce is sharing this information through Salesforce-to-Salesforce Connection, which is a Salesforce connectivity method that is controlled by ITA to securely share records with EXIM Bank without any data loss. PII such as Case Owner (ITA employee Name), Contact (External) and Contact Email (External) are shared with EXIM Bank and BII such as Organization / Account Name, Organization / Account City, Organization / Account Country, Organization / Account County, Organization / Account State, Organization / Account Street are shared with EXIM Bank.

Privacyshield / Participation App

ITA is sharing following PII information through their publicly accessible website (https://www.privacyshield.gov/).
Client Name, Client Email, Client Country, Client Postal Code, Client Address, Client Street, Client City, Client State, Client Postal Code, Client Country, Client Phone, Client Fax, Client Title and Client Email.

And following BII information through their publicly accessible website
Organization / Account Name, Organization / Account Street, Organization / Account City, Organization / Account State, Organization / Account Zip Code (5 digit), Organization / Account Country, Organization / Account Privacyshield Certification, Organization / Account Privacyshield Participation Status, Organization / Account Privacyshield Covered Data, Organization / Account Privacyshield Dispute Resolution Type.

Toolkits App

ITA is sharing no PII information for Toolkits.
ITA is sharing through following BII information their publicly accessible website (https://www.privacyshield.gov/).
Client Name, Client Email, Client Country, Client Postal Code, Client Address, Client Street, Client City, Client State, Client Postal Code, Client Country, Client Phone, Client Fax, Client Title and Client Email.
And following BII information through their publicly accessible website
Organization / Account Name, Organization / Account Toolkits Solutions.

Web App
No PII / BII information is shared publicly.

Knowledge App
No PII / BII information is shared publicly.

ADCVD
No PII / BII information is shared publicly

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

Legal authority to collect PII and/or BII is contained in the following laws or Executive Orders as it may apply: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O.
131614; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; E.O. 12554; Public Law 100-71, July 11, 1987.

15 U.S.C. Sec. 1512; 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); 31 U.S.C. 3711; 5 U.S.C. App.—Inspector General Act of 1978, § 2; 5 U.S.C. App.—Reorganization Plan of 1970, § 2; 13 U.S.C. § 2; 13 U.S.C. § 131; 15 U.S.C. § 272; 15 U.S.C. § 1151; 15 U.S.C. § 1501; 15 U.S.C. § 1516; 15 U.S.C. § 3704b; 16 U.S.C. § 1431; 35 U.S.C. § 2; 42 U.S.C. § 3121 et seq.; 47 U.S.C. § 902; 50 U.S.C. App. § 2401 et seq.; E.O. 11625; 77 FR 49699 (Aug. 16, 1012); 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

(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):					

x_ 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 (version 01-2015 or 01-2017).

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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	x	l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID	x				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	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	x	r. Criminal Record	
e. Age		l. Email Address	x	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	x	i. BusinessAssociates	x
b. Job Title	x	f. Salary		j. Proprietary or Business Information	
c. Work Address	x	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data(specify):					

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	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address	x	f. Queries Run	x	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources

Within the Bureau	x	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 isensured.

Salesforce data is collected through Online web forms entered directly by external individuals or entered manually by ITA Users who receive the information directly from the individuals.

2.4 Is the information covered by the Paperwork ReductionAct?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
x	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):			

x	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. *(Checkall that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	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, ordisseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	x
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	x	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	x	For web measurement and customization technologies (multi-session)	x
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).

ITA, primarily through Export program participants, collects the data fields listed in section 2.1 to assist customers in connecting with business assistance services, programs, data, and other resources in a larger effort to help the economy by supporting small and medium sized businesses and exporters financial growth. The information collected includes information associated with clients' participation for services, collection of any fees (through pay.gov), monitor performance, provide client information to federal agencies and bureau partners to better serve the customer.
The following modules process
PII: CRM:
CRM is a module used to manage relations between ITA, and the Organizations and Individuals interested in working with the ITA. This is an internal application, accessible only to ITA employees, who collect the information from external perspective clients through In-Person contact, Phone or email. Individuals can contact the ITA to provide, access, update or amend their information.
PrivacyShield:
Information in Privacy Shield is collected through Online forms by/after registration and the individuals can login to their community and update their PII/BII information. The Privacy Shield App is administered by ITA / U.S. Department of Commerce and enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from determinations whether data are secured to an adequate level of acceptance.
ToolKits:
Toolkits allows U.S. Exporters to learn about the global challenges, including those related to standards and regulations, facing select U.S. industries from the latest ITA Top Markets Report for the sector. The toolkits also include contact information for ITA industry analysts who are knowledgeable about global conditions in their sector of expertise. Information is collected through Online forms by/after registration and the Individuals can login to their community and update their PII/BII information.

ADCVD

The Antidumping Duty and Countervailing Duty (AD/CVD) Case Management System is an internal application built on the Salesforce Platform. This application consists of data modeling, date calculations/automation, staffing and reporting/dashboards. Enforcement and Compliance (E&C) users currently engage with system by creating and staffing cases, inputting dates/Federal Register information and reviewing dashboards/reports, in order to successfully make it through their business process before a deadline passes. Only available to ITA Employees with the need-to-know.

No PII is collected.

Qualtrics is a Survey System we integrated with Salesforce to send out surveys to Contacts (External Client) upon Closing following types of Case in CRM App:

- Export Promotion
- Commercial Diplomacy
- Investment Promotion

Once the Case Owner (ITA Employee) Closes one of the Cases – Salesforce will trigger an **Outbound message** to **Qualtrics** to send out the survey to the **Case Contact** (External Client).

Survey Questions has been mapped with Salesforce fields:

Survey Number - Autonumber
Case Owner - ITA Employee
Primary Contact - ITA Employee
Contact - External Client
Case - Related Salesforce Case Number
Record Type - Type of Survey
Likely to Recommend - Survey Question
Objectives Met - Survey Question
Type of Information - Survey Question
Better Serve - Survey Question
Best Working with Us - Survey Question

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.)

Insider threats are addressed through Annual Cybersecurity Awareness Training and Salesforce specific training for systems users is conducted in order to communicate the appropriate procedures for handling and dispensing of information. System is maintained in areas accessible only to authorized personnel in a building protected by security guards. System is password protected and is FIPS 199 compliant. All records are retained and disposed of in accordance with Department directives and series records schedule. As previously noted, Pay.gov is completely external to Salesforce; users are forwarded out of the Salesforce environment and on to Pay.gov for any necessary payments/transactions.

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	x		
DOC bureaus	x		
Federal agencies	x		
State, local, tribal gov't agencies			
Public	x		
Private sector			
Foreign governments			

Foreign entities			
Other (specify):			

	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.
x	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:
x	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	x	Government Employees	x
Contractors	x		
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.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. Specific SORN: ITA-8 Salesforce Relationship Management System; http://osec.doc.gov/opog/PrivacyAct/SORNs/ita-8.html http://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html	
x	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.export.gov/website-privacy-act / https://www.privacyshield.gov/website-privacy-act.	
x	Yes, notice is provided by other means.	Specify how: Specify how: Notification is provided in different means depending on the application. **CRM:** Individuals are notified verbally to ITA POC. **Web App:** Not collecting, maintaining, or disseminating PII/BII. **Knowledge App:** Not collecting, maintaining, or disseminating PII/BII. **Privacyshield /Participation App:** Individuals received notice prior to registration. **Toolkits App:** Individuals received notice prior to registration. **AD/CVD:** Not collecting, maintaining, or disseminating PII. **Qualtrics Survey System:** Users have the option to submit survey responses anonymously or share their identity to DoC/ITA.
	No, notice is not provided.	Specify why not:

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

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Specify how: Yes, Individuals have an opportunity to decline to provide PII/BII. The manner is dependent on the application. **CRM:** Individuals can decline verbally directly to ITA POC. **Web App:** Not collecting, maintaining, or disseminating PII/BII. **Knowledge App:** Not collecting, maintaining, or disseminating PII/BII. **Privacy shield /Participation App**: Individuals have the opportunity to decline at time of registration although this may affect the ability to self-certify to the frameworks discussed above. **Toolkits App:** Individuals have the opportunity to decline at time of registration. **AD/CVD:** Not collecting, maintaining, or disseminating PII. **Qualtrics Survey System:** Users have the option to submit survey responses anonymously or share their identity to DoC/ITA.

	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Privacy statement link is displayed in the registration page for these applications: **CRM:** Individuals have the opportunity to consent verbally to ITA POC **Web App:** Not collecting, maintaining, or disseminating PII/BII. **Knowledge App:** Not collecting, maintaining, or disseminating PII/BII. **Privacyshield /Participation App:** Individuals have the opportunity to consent at time of registration. **Toolkits App:** Individuals have the opportunity to consent at time of registration. **ADCVD:** Not collecting, maintaining, or disseminating PII. **Qualtrics Survey System:** Users have the option to submit survey responses anonymously or share their identity to DoC/ITA.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **CRM:** This is an internal app and accessible only to internal ITA employees, who collect the information from External Clients through In-Person, Phone or email. Individuals can contact the ITA to access, amend or update their information. **WebApp:** Not collecting, maintaining, or disseminating PII/BII. **Knowledge App:** Not collecting, maintaining, or disseminating PII/BII. **Privacyshield / Participation App:** Information is collected through Online forms by/after registration and the Individuals can login to their community and update their PII/BII information. **Toolkits:** Information is collected through Online forms by/after registration and the Individuals can login to their community and update their PII/BII information. **ADCVD:** Not collecting, maintaining, or dissemination PII/BII. **Qualtrics Survey System:** Information is collected through Online forms by/after registration and the Individuals can login to their community and update their PII/BII information.

	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

x	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: This requirement is addressed by the following implemented Auditing controls: AU-2 It was determined from an interview with salesforce administrator and a screen shot provided that salesforce can monitor events that affect the confidentiality of PII, such as unauthorized access to PII. "View Setup Audit Trail" and " Log in History" AU-3 SalesForce generates audit records by several event categories AU-6 It was determined through an interview with Salesforce Adm and a screenshot provide that Salesforce can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
x	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): August 11, 2020
	☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J 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).
x	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
x	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).*

FedRAMP Approved Salesforce Gov system employs a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in-transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited, to the following:

- Intrusion Detection I Prevention Systems (IDS I IPS)
- Firewalls
- Use of trusted internet connection (TIC)
- Anti-virus software to protect host/end-user systems
- HSPD-12 compliant PIV cards
- Access controls

Section 9: Privacy Act

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

x_ 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."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: ITA-8 Salesforce Relationship Management System; http://osec.doc.gov/opog/PrivacyAct/SORNs/ita-8.html
	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.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: ITA Salesforce platform follows 10 years of data/record retention as part of the Salesforce contract.
	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:
x	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	x
Other (specify):			

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.
x	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.)*

x	Identifiability	Provide explanation: We collect information like Name, email, Telephone Number. All of this information has a low sensitivity level

x	Quantity of PII	Provide explanation: CRM is used to work with individuals interested in working with ITA. As such there is a great volume of PII collected from individuals and can include approximately 400,000+ Records (most are CRM Contacts with Name, Emails and phone number) Although data elements are limited, there is a quantity of information.
	Data Field Sensitivity	Provide explanation:
x	Context of Use	Provide explanation: The use context depends on the application: (For example CRM: the PII relates to a Contact who is interested to work with ITA) so the information is limited to the online registration form requirements. The same is for Toolkit. PrivacyShield requires a self-certifying organization to provide essential information but no more than required.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: In ITA Salesforce Org (GovCloud)
x	Other:	Provide explanation: Website (Some information is displayed in Website as part of business functionality like privacyshield.gov/list)

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.)

No potential threats to privacy were discovered.

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:
x	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:
x	No, the conduct of this PIA does not result in any required technology changes.