

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



**Privacy Threshold Analysis
for the
ITA Salesforce Platform (ITA_SFPP)**

U.S. Department of Commerce Privacy Threshold Analysis

International Trade Administration Salesforce Platform

Unique Project Identifier: 2520

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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), Privacy Shield 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 serving agency. 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

Web App PII/BII

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
- Trade Agreements

Knowledge App PII

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

Privacy Shield / 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](https://www.privacyshield.gov) website) and publicly commit to comply with the Framework's requirements. The self-certified companies will be reviewed by the Privacy Shield 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.gov](https://www.privacyshield.gov) website.

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 Privacy Shield List URL - <https://www.privacyshield.gov/list> , and BII information is searchable through Privacy Shield 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

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.

***ADCVD PII**

No PII is collected.

Qualtrics

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).

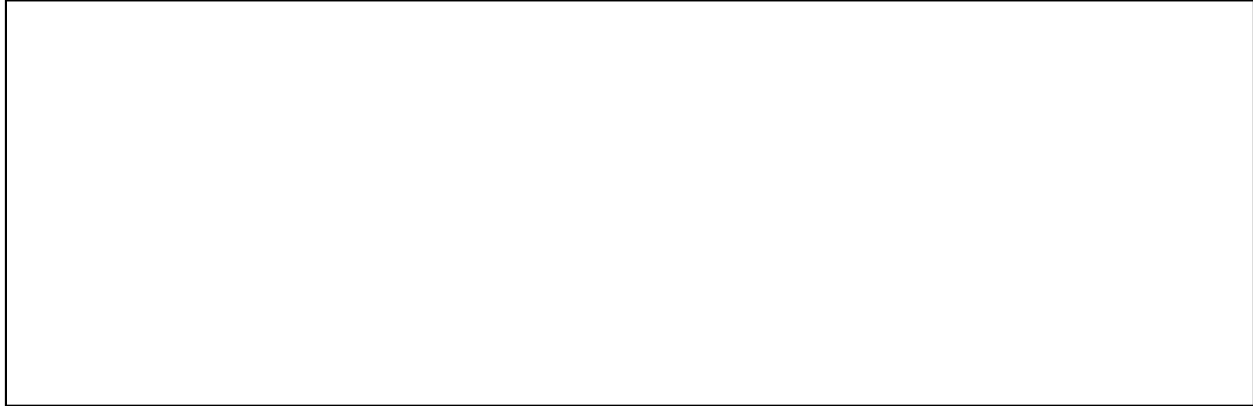
Qualtrics Survey Questions has been mapped with Salesforce fields:

- 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>



Address the following elements:

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

Salesforce Platform is a major application.

b) *System location*

Cloud-hosted system in FedRAMP approved Salesforce Government Cloud

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

Interconnects with Pay.gov (Privacy Shield App Payment System) and US Exim Bank (Salesforce-to-Salesforce Connection -Elastic Search)

d) *The purpose that the system is designed to serve*

ITA Salesforce Platform (ITA SFPPF) was designed to create a unified, enterprise-wide view of customers while presenting a single “face” to the customer. It allows all ITA staff across different business units to effectively collaborate and share customer information, regardless of their physical location. Additionally, SFPPF enables the Office of Domestic Operations (ODO) and the Office of International Operations (OIO) trade specialists to see client information for all networks and posts in one system.

e) *The way the system operates to achieve the purpose*

For administrative matters, improvement of Federal services online, to promote information sharing initiatives, and for web measurement and customization technologies (single session/multi-session).

f) *A general description of the type of information collected, maintained, used, or disseminated by the system*

Salesforce stores/collects information such as: Name, Telephone Number, Email Address, Business Address, Title. These are collected through online entry (via various applications/modules) or manually entered by ITA employees (for CRM purposes). These data types are maintained under standard ITA policy and are only accessible for authorized users.

g) *Identify individuals who have access to information on the system*

System admins (full Admin rights); Internal Users (limited rights with role-based access);
Community Users (limited rights for interaction with ITA)

h) *How information in the system is retrieved by the user*

Information is retrieved via an online/web connection

i) *How information is transmitted to and from the system*

Online entry with some automation in use using secure HTTPS Connection (SC-8) - HTTPS security (TLS 1.2) for data transmission.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

This is a new information system. *Continue to answer questions and complete certification.*

This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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 a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). Continue to answer questions and complete certification.

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). Skip questions and complete certification.

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

Yes. This is a new information system.

Yes. This is an existing information system for which an amended contract is needed.

No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. (Check all that apply.)

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

No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)”

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- DOC employees
- Contractors working on behalf of DOC
- Other Federal Government personnel
- Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

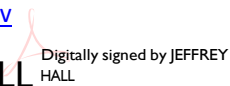
No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X The criteria implied by one or more of the questions above **apply** to ITA Salesforce Platform and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

 The criteria implied by the questions above **do not apply** to the ITA Salesforce Platform and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner</p> <p>Name: Jeffrey Hall Office: ITA/OCIO/PDD Phone: 202-482-4934 Email: Jeffrey.g.Hall@trade.gov</p> <div style="text-align: center;">  <p>JEFFREY HALL <small>Digitally signed by JEFFREY HALL Date: 2022.03.28 13:44:05 -04'00'</small></p> </div> <p>Signature: _____ Date signed: _____</p>	<p>Information Technology Security Officer</p> <p>Name: Joe Ramsey Office: ITA/OCIO/CRMD Phone: 202-482-2785 Email: joe.ramsey@trade.gov</p> <p>Signature: _____ Date signed: _____</p>
<p>Privacy Act Officer</p> <p>Name: Chad Root Office: ITA/OCIO/CRMD Phone: 202-482-1883 Email: chad.root@trade.gov</p> <p>Signature: _____ Date signed: _____</p>	<p>Authorizing Official</p> <p>Name: May Cheng Office: ITA/OCIO/DCIO Phone: 202-482-3801 Email: may.cheng@trade.gov</p> <p>Signature: _____ Date signed: _____</p>
<p>Bureau Chief Privacy Officer</p> <p>Name: Chad Root Office: ITA/OCIO/CRMD Phone: 202-482-1883 Email: chad.root@trade.gov</p> <p>Signature: _____ Date signed: _____</p>	