Template Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Trade Agreement Secretariat (TAS) e-Filing

U.S. Department of Commerce Privacy Threshold Analysis

Trade Agreement Secretariat (TAS) e-Filing

Unique Project Identifier: 2729

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

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

b) *System location*
Application hosted in Microsoft Azure

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

d) *The purpose that the system is designed to serve*
The TAS e-Filing system will be a new online system for use by TAS and FTA partners to manage trade disputes from initiation through resolution. The system will grant access to all interested parties, — governmental and private — to dispute documentation, managing viewing rights to ensure that proprietary information is protected. The new system will also oversee dispute workflow, allowing administrators to easily assign actions and deadlines, and provide notifications as necessary. There will be a feature allowing the general public to search and view all non-sensitive information and documentation related to disputes. For TAS and its counterparts in other agreement-signatory countries, there will be reporting and analysis functions, allowing these users to perform searches, track all activity around disputes, and create reports to analyze individual disputes and overall system usage. TAS e-Filing will be fully capable of managing United States-Mexico-Canada Agreement (USMCA)

disputes on launch, and will be developed under the assumption that it can be expanded to meet the requirements of other FTAs to which the United States is a Party.

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

• All users required to participate and provide materials for proceedings will be able to create accounts to use the system and supply documents as necessary.

• The system will be a central repository for all documents related to a dispute. It will keep those documents logically organized, showing revisions and approval actions, as well as keeping parallel proprietary and redacted non-proprietary versions of the same document.

• The system will allow TAS and its non-US counterparts to easily manage workflow for all users involved in a dispute. They will be able to request submission and approvals, setting and altering deadlines. Many aspects of workflow can be automated, alleviating the need for labor-intensive processes. Notifications of needed actions will be sent to parties as necessary.

• Access to documents will be tightly controlled based on the identity of users. The system will meet or exceed required security standards. Access to proprietary information will be restricted to approved users.

• A key component of the new platform will be public access to a digital "reading room.". Members of the general public could create guest accounts, which could be approved upon email validation. With these accounts, people will be able to search for and view materials related to FTA disputes, but limited to only those documents without proprietary or otherwise sensitive information.

• TAS and its counterparts will be able to perform searches, compile information, and analyze data system-wide as well as relating to an individual dispute. They will have the ability to view data online or export into other formats (e.g., Word, Excel).

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

Information collected and disseminated: filing, briefings, and other documents related to disputes; billings/invoices from panelists; "Public PII" information about account holders (e.g., email address, name, company/organization); statistics/metrics related to system usage; document download/views.

1.) ITA Authenticated Users and external entities access the TAS e-Filing system through the web front end application. Authentication will be handled by Azure B2C, a fully managed identity management service that integrates with other ID providers like login.gov.

2.) Secured Web API is used to limit access and functionality of the logged in user. Each user has a role assigned which limits access to specific tasks and functions of the application. In addition, the application will have a public access component that allows read-only access to documents and cases as allowed by the application administrators.

3.) Authorized ITA users will set access policies for each case in the application.

g) *Identify individuals who have access to information on the system*
Information access will be controlled based on the identity of the user; the system will control permissions to ensure information can only be seen by users with the right to see it. User access to any non-public information will be approved by ITA staff.
Full Access
- *Trade Agreement Secretariat (office within ITA): full access includes certain administrative controls*

Limited Access –t
- *U.S. Government officials from US Trade Representative, U.S. International Trade Commission, and Enforcement & Compliance*
- *Attorneys (Panelists, Assistants, Private Attorneys)*
- *Foreign government officials*

Very Limited Access*:*
- *Members of the public*

h) *How information in the system is retrieved by the user*
Users log into system using an account. Able to view information in the system and download certain documents.

i) *How information is transmitted to and from the system*
Users upload information and documents into the system using forms or other interfaces.

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 not a SAOP approved Privacy Impact Assessment. *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 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

_X__ 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.

__X_ 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.

__X__ Yes. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Judicial proceedings (audit recordings and written transcripts)			

____ 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.)."

__X__ 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."

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

__X__ DOC employees
____ Contractors working on behalf of DOC
__X__ Other Federal Government personnel
__X__ 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.

_X___ 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?

__X__ 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.

__X__ 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__ I certify the criteria implied by one or more of the questions above **apply** to the Trade Agreement Secretariat (TAS) e-Filing and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Trade Agreement Secretariat (TAS) e-Filing and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Michael Hunt Office: TSI-Enterprise Apps Phone: 202-482-6552 Email: Michael.Hunt@trade.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Michael Hunt Digitally signed by Michael Hunt Date: 2021.11.23 12:16:16 -05'00' Date signed:	**Information Technology Security Officer** Name: Joe Ramsey Office: TSI IS Phone: 202-482-2785 Email: joe.ramsey@trade.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JOSEPH RAMSEY Digitally signed by JOSEPH RAMSEY Date: 2021.12.01 10:22:11 -05'00' Date signed:
Privacy Act Officer Name: Chad Root (Acting) Office: TSI IS-Comp Phone: 202-482-1883 Email: chad.root@trade.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.10.22 11:25:12 -04'00' Date signed:	**Authorizing Official** Name: Rona Bunn Office: TSI CIO-DCIO Phone: 202-482-9104 Email: rona.bunn@trade.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: RONA BUNN Digitally signed by RONA BUNN Date: 2021.12.01 11:52:00 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Chad Root (Acting) Office: TSI IS-Comp Phone: 202-482-1883 Email: chad.root@trade.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.10.22 11:25:32 -04'00' Date signed:	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.