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

International Trade Administration/ Trade Agreement Secretariat (TAS) e-Filing System

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
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 system

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

The TAS e-Filing application is a dynamic case management application designed for use by the Trade Agreements Secretariat (TAS). The purpose of the application is to manage dispute matters handled by that office. The system will allow the submission and processing of such disputes to include collecting case information, managing files, assigning tasks, along with other related functionality, from case initiation through resolution. This application also facilitates the USMCA directive to process all disputes electronically.

All filings that are public documents will be made available to individuals, via the public reading room, that create a TAS E-filing system account and agree to the TAS E-filing User Agreement. Furthermore, users that have a requested elevated permissions to become a dispute participant within the TAS E-filing system, and those permissions have been granted by TAS, will be able to access public documents of the dispute they are a participant of under the dispute section of the system as well.

All dispute participants whom wish to access business proprietary information in a USMCA or NAFTA dispute must receive approval from the investigating authority associated with the dispute. In order to receive this approval, a dispute participant is required to submit an administrative protective order (APO) with the respective investigating authority. The respective investigating authority will then review the dispute participant's APO application and either approve or reject the application. If the application is rejected, the dispute participant will not receive access to the dispute documents that contain BII. If the application is approved, the respective investigating authority will notify the respective secretariat and the dispute participant of the approval of the application.

Within the TAS E-filing system, the respective secretariat will then manually grant the dispute participant access to the dispute documents containing BII for which their application was approved for. The dispute participant will continue to have access to the dispute documents containing BII until they request be removed or a dispute is completed/terminated. Once a dispute is completed or terminated, the BII documents will be deleted from the system, in accordance with the investigating authorities APO. In addition, the investigating authority could request that the dispute participant's access be withdrawn. This process is the same for Canadian and Mexican entities; they just have different APO request forms that are specific to and approved by their respective investigating authorities.

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

TAS e-Filing handles trade disputes for parties involved in the US-Mexico-Canada (USMCA) trade agreement. These disputes include legal filings that may contain BII for companies based in these countries.

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

There are nine (9) different types of user roles for the system.

- TAS Admins (Internal)
- Foreign Government Secretariats (External)
- Investigating Authorities (E&C and USITC) (Internal/External)
- Other US Government officials (External)
- Private Attorneys (External)
- Other Individuals Assisting with Administration of Disputes (Internal/External)
- Members of the Public (External)
- Panelists and Assistants (External)
- TSI Personnel/Admins (Internal)

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

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

i) How information is transmitted to and from the system

Data is uploaded by users directly to the application through a public interface, which is encrypted by SSL and TLS 1.2. There are no external systems that connect to the TAS e-Filing system. There is no transmission to or from the system to other applications.

Questionnaire:

1. Status of the Information System

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

__X__ 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.*

____ 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?

__X__ 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.

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

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): It is possible that audio recordings of public disputes related to trade cases will be uploaded into the TAS e-Filing system.			

____ 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.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ 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 TAS e-Filing System 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 TAS e-Filing System 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 Signature: Michael Hunt Digitally signed by Michael Hunt Date: 2020.12.17 17:15:47 -05'00' Date signed:	**Information Technology Security Officer** Name: Joe Ramsey Office: TSI IS Phone: 202-482-2785 Email: joe.ramsey@trade.gov Signature: JOSEPH RAMSEY Digitally signed by JOSEPH RAMSEY Date: 2020.12.18 09:28:27 -05'00' Date signed:
Privacy Act Officer Name: Chad Root (Acting) Office: TSI IS-Comp Phone: 202-482-1883 Email: chad.root@trade.gov Signature: Chad Root Digitally signed by Chad Root Date: 2020.12.17 18:10:38 -05'00' Date signed:	**Authorizing Official** Name: Rona Bunn Office: TSI CIO-DCIO Phone: 202-482-9104 Email: rona.bunn@trade.gov Signature: RONA BUNN Digitally signed by RONA BUNN Date: 2020.12.18 20:26:08 -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 Signature: Chad Root Digitally signed by Chad Root Date: 2020.12.17 18:10:52 -05'00' Date signed:	