Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Trade Agreement Secretariat (TAS) e-Filing

Reviewed by: TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.10.22 11:28:03 -04'00' _____, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.10.22 11:48:12 -04'00' 1/12/2022

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

U.S. Department of Commerce Privacy Impact Assessment
[International Trade Administration/Name of IT System]

Unique Project Identifier: 2729

Introduction: System Description

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
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 way the system operates to achieve the purpose(s) identified in Section 4
• 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).

(e) 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.

(f) How information is transmitted to and from the system
Information is transmitted using TLS 1.1 approved encryption.

(g) Any information sharing conducted by the system
System is standalone, it does not share information with any other systems.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
This information is collected pursuant to 19 U.S.C. §§ 3315, 3431 – 3438, 4515, 4581 – 4601, 4691 – 4693, 4714. These cover NAFTA and USMCA and are what we cited to in our User Agreement. 19 CFR part 356 is another authority. It currently covers the procedure and rules for implementing Article 1904 of NAFTA, and it is where the procedure and rules for implementing Article 10.12 of USMC.

(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-		e. New Public Access		h. Internal Flow or	

Anonymous				Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

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

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

_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).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID	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		r. Criminal Record	
e. Age		l. Email Address		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. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X

c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

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		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

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

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

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign	X		
Other (specify): Contributions could come from Canadian or Mexican government according to each dispute.					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Canadian and Mexican private legal and corporate entities can contribute information per dispute and according to APO.					

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

All information that is forward facing to users of the system can be manually updated by the TAS team and/or TSI through administrative controls built into the system to ensure that all information being displayed to users is accurate and up to date. In addition, information that a user would submit into the system, for example their contact information, can also be updated by the TAS team upon the request of the user. Furthermore, any filing submitted by a user is checked for accuracy by the TAS team to ensure that the user has associated the filing with the correct metadata in the system prior to the document being made available to other users.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
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. *(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.			

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

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Court Cases, disputes between parties to US Trade Agreements according to negotiated access in those agreements. These disputes are brought by both private entities and government entities. Public individuals can see the basics of disputes as they are made official, and access to public documents. Access to BII is controlled via APO and dependent on a user's role in the system on a case by case basis.			

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).

PII is collected from a user when they first create their account. This information is collected to by the TAS E-filing system to identify for what means the user is using the system. Without collecting the name and email of a user, we would be unable to identify whom is who in the system, which will be needed when we are granting specific users' higher levels of access to system – users that will be filing documents and users that will be viewing documents containing business proprietary information (BPI). In addition, if a document were to be filed as a public but the filer forgot to remove a piece of BPI in the filing which was then displayed to public users within the system, we would have the contact information of all users to notify them to destroy that document.

BII is collected to be able to build out the service lists of dispute participants within the system. We would note that all service lists for disputes that TAS administers are public documents. In addition, all the BII we are collecting has already been collected by the investigating authority for their investigation and determination, and this information is made available to the public by the investigating authority.

Business proprietary information (BPI) is submitted through the same process as a public

document; however, there is an important distinction in that all filings will be defaulted to containing BPI. Thus, if a user is filing a public document, they must actively indicate that the document is public, or the system will treat the document as if it contains BPI. In handling a document with BPI, the system automatically restricts user access to the document, in that only users with an approved APO for the specific dispute, issued by the investigating authority of that dispute, can access the document containing BPI. An important note here is that APO's are issued on a dispute-by-dispute basis, thus access to documents in the system containing BPI is also issued on a dispute-by-dispute basis. Furthermore, once a dispute has been completed or terminated, all documents associated with that specific dispute containing BPI will be destroyed, in accordance with the APO issued and approved by the investigating authorities.

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.)

The most notable potential threat to privacy in the TAS E-filing system is BPI becoming public. An initial note here is that all users that have access to BPI have an agreement with the respective investigating authority to view that investigating authorities BPI and use it in the filings (dispute participants).

All dispute participants who 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 BPI. 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 BPI for which their application was approved for. The dispute participant will continue to have access to the dispute documents containing BPI until they request be removed or a dispute is completed/terminated. 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.

However, if BPI was incorrectly filed and labeled as public, TAS would immediately restrict the public's access to the document by changing its metadata from public to proprietary. It would then be on the filer to amend this submission by refiling a corrected document. Thus, TAS would not be individually correcting a document nor disseminating it. However, TAS would be able to

send all users in the system a notification of the error indicating that if they accessed this document while it is was public, they should destroy it.

Section 6: Information Sharing and Access

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

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector	X		
Foreign governments	X		
Foreign entities	X		
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?

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

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

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
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): Members of the public have access to the TAS system but will only see non-sensitive information deemed publicly available. They will NOT see any of the BII or PII in the system.			

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.	
	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: _____.	
X	Yes, notice is provided by other means.	Specify how: User Agreement published, accepted and recorded on registration in the application. See Appendix. https://tas.trade.gov
	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: In order to submit documents to pursue a dispute under the TAS jurisdiction, BII will be included. If they decline, their role in the system is limited to public only

		documents and information.
	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: Individuals can provide a BII version of a document to be used in a dispute within the negotiated agreement of USMCA
	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: Users would have to reach out to TAS administrators to change/update PII (ie misspelling of name during creation of user account).
	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: All documents submitted to the system is tracked from upload, review, approval, docketing, and download by user, date and time. A document log is maintained within the system
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): __1/6/2021_____ ☐ 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.
X	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).*

Data is encrypted in transit and at rest – the system utilizes SSL and TLS1.2 connection for data in transit and inherits data at rest encryption from Microsoft Azure. Access to BPI is dependent on the role a user is assigned in the system.

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)*: COMMERCE/DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
	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: DAA-GRS2013-0003-0001 36
	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	X	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.)*

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

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

X	Identifiability	Provide explanation: Can trace users who have accessed specific documents within the system
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: Covered under the APO process

X	Obligation to Protect Confidentiality	Provide explanation: Covered under the APO process
X	Access to and Location of PII	Provide explanation: Only authorized users can access any BII
	Other:	Provide explanation:

Section 12: Analysis

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

The agreement between Canada, Mexico and The United States governs the types and quantity of information collected to complete any disputes addressed by the Trade Agreements Secretariat. The information collected is only relevant to the dispute brought before the Trade Agreement Secretariat and the Parties who participate in the dispute management.

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.