Template Version Number: 12-2022

U.S. Department of Commerce
International Trade Administration
Office of Chief Information Officer (ITA OCIO)

Privacy Impact Assessment
for the
OTEXA

Reviewed by: Chad Root, Bureau Chief Privacy Officer (BCPO)

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.02.27 14:14:58 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce Privacy Impact Assessment
ITA OTEXA

Unique Project Identifier: 2574

Introduction: System Description

Provide a brief description of the information system.

The Free Trade Commercial Availability section of the Office of Textiles and Apparel (OTEXA) portal allows OTEXA staff to process requests to determine whether specific fibers, yarns, or fabrics are not available in commercial quantities in a timely manner from designated trade partner countries. Trade partner countries include Australia, Bahrain, Chile, Colombia, Korea, Morocco, Panama, Peru, Singapore, and member countries of the US, Mexico, Canada (USMCA) trade agreement and member countries of the Dominican Republic-Central America Free Trade Agreement (CAFTA-DR). OTEXA, on behalf of the Chairman of Committee for the Implementation of Textile Agreements (CITA), processes all such requests and the Chairman makes recommendations to CITA, in accordance with the procedures published by CITA. The portal also provides public access for interested parties to a list of products that have been determined to be commercially unavailable, as well as a searchable database of past requests.

OTEXA's Made in the USA Sourcing and Products Directory assists buyers in sourcing U.S.-made textile, apparel, and footwear products from U.S. vendors, which include manufacturers, suppliers, distributors, and producers. To qualify for a listing in this directory, a vendor must be a company incorporated in the United States with at least one manufacturing plant, assembly plant, or distribution center that manufactures, assembles, or distributes U.S.-made textile, apparel, or footwear products while listed in the directory. All information on the directory is public, does not contain any personally identifiable, however, OTEXA Commercial Availability and The Earned Import Allowance Program (EIAP) does process business confidential information, and the company listings are created by the companies themselves.

The Earned Import Allowance Program (EIAP) provides duty-free entry for certain apparel from Haiti into the United States. For every two square meter equivalents (SME) of qualifying fabric, one SME may enter the U.S. duty-free using third party yarn and fabric. OTEXA's EIAP online system assists qualifying producers (Company) in keeping a record and issuing certificates that are used by U.S. Customs and Border Protection (CBP) for duty-free entry of EIAP-qualifying apparel.

Address the following elements:

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

(b) System location
OTEXA is located in ITA's Azure tenant (Microsoft Azure East)

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
OTEXA has two interconnections. OTEXA interconnects to ITA's Azure platform and OTEXA EIAP Haiti interconnects with U.S. Customs and Border Protection (CBP).

(d) The way the system operates to achieve the purpose(s) identified in Section 4
For Administrative Matters – Made in the USA helps US based businesses advertise their services to buyers and consumers looking to source US made goods and services.

To Improve Federal Services Online – EIAP allows businesses to track and manage earned import credits that are given by the US government related to qualifying textile imports from Haiti.

To Promote Information Sharing Initiatives – Made in the USA allows buyers and consumers the ability to directly source goods and services from US based companies. Commercial Availability allows individuals to see updated trade agreements related to textile and apparel goods from participating countries.

For Employee and Customer Satisfaction – Made in the USA helps with customer satisfaction for buyers and consumers who wish to source and procure US based goods and services specifically.

(e) How information in the system is retrieved by the user
Commercial Availability:
Users access the OTEXA Commercial Availability site via web browser at the following URL: https://www.trade.gov/otexa-fta-commercial-availabilty. This site is a fully publicly accessible site with no user account or authentication required.

Made in the USA:

Users access the OTEXA Made in the USA site via web browser at the following URL: https://www.trade.gov/made-usa-directory

Businesses can sign up to register as a company and create a company profile that is searchable by the public. Made in the USA uses Azure B2C for account creation and to sign in and authenticate businesses with accounts.

Public users can view the profiles of all registered businesses. Public users are not required to create an account or authenticate to the site to view published business information.

The Earned Import Allowance Program (EIAP):

Users access the OTEXA EIAP site via web browser at the following URL: https://www.trade.gov/haiti-earned-import-allowance-program

Businesses can create an account to submit a request for a deposit, redeem credits for import certificates, and review account balances and activity. EIAP uses Azure B2C for account creation and to sign in and authenticate businesses with accounts.

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

Information for all aspects of OTEXA is transmitted to and from the system via web browser. All data is encrypted in transit and at rest. The system utilizes SSL and TLS 1.2 connections for data in transit and inherits data at rest encryption from Microsoft Azure.

(g) Any information sharing

OTEXA's Haiti EIAP system does share information with CBP.

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

a. Commercial Availability

i. Section 203(o)(4) of the CAFTA-DR Implementation Act; the Statement of Administrative Action ("SAA"), accompanying the CAFTA-DR, at 16-20.

ii. Section 203(o) of the Implementation Act and Proclamation No. 8818, 77 FR 29519 (May 18, 2012).

iii. Section 203(o) of the Implementation Act and Proclamation No. 8894, 77 FR 66507 (November 5, 2012).

iv. Section 203(o) of the US-PERU TPA and Proclamation No. 8341, 74 FR 4105 (Jan. 22, 2009).

b. OTEXA Haiti EIAP: The Food, Conservation, and Energy Act of 2008 (FCEA of 2008) (Pub. L. No. 110-246), as amended by the Haiti Economic Lift Program Act of 2010 (Pub. L.

No. 111-171). The FCEA of 2008 requires that the Secretary of Commerce establish an EIAP under the Caribbean Basin Economic Recovery Act (CBERA). The Secretary of Commerce has delegated his authority under the FCEA of 2008 to implement and administer the EIAP to OTEXA.

(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.
__X__ 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): ITA OTEXA has been operational since 1/21/2021. However, due to administrative oversight, previous versions of the ITA OTEXA PIA have not been reviewed and approved by the DOC SAOP.					

____ 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.

___ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

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): Importer of Record Number					
*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. Marital Status	
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		f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Names and locations of suppliers.					

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		e. ID Files Accessed	
b. IP Address		f. Queries Run		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 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	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign	X		
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

For Haiti EIAP and Commercial Availability, users are asked to attest to the accuracy of the information prior to submission. For Made in USA, OTEXA staff vet the applicants to confirm their suitability for inclusion in the directory.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. Only applies to certain commercial availability filings: OMB 0625-0265, 0625-0272, and 0625-0273.
	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		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, or disseminated. *(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	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
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).

Made in the USA – Business contact related PII is collected directly from a business representative to register an account and publish their information directly to the Made in the USA site directory for consumers to view. This information is used for buyers/consumers to source US made products and services from US vendors at each step of the textiles, apparel, footwear, and travel goods supply chain. All PII collected relates only to businesses.

EIAP – Business contact related PII is collected directly from a business representative to register and account in EIAP to manage and view earned import credits for certain apparel imported from Haiti. All PII collected relates only to businesses.

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 OTEXA system is PII/BII becoming public. This threat is mitigated by having security guidelines in place. Access controls (ie only authorized users, BII collection portal/database not publicly available), audit measures in place and log review monitoring system access/activity, annual CSAT training to discourage insider threats.

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			
Federal agencies	X	X	
State, local, tribal gov't agencies			
Public			X
Private sector			X
Foreign governments			X

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Foreign entities			
Other (specify): Selected companies	X		X

	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.

X	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: U.S. Customs and Border Protection (CBP) The interconnection between CBP/DOC ITA network connected through the CBP ICP are supported by Multiprotocol label switching (MPLS) at the ICP. DHS OneNet transport services utilize MPLS and Dynamic Multipoint Virtual Private Network (DMVPN) technologies. The CBP ICP provides WAN Connectivity services, Internet services, and perimeter security protection to the CBP ACE system. It also uses TLS 1.2 for encryption.
	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.)*

	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:	
	Yes, notice is provided by other means.	Specify how:
x	No, notice is not provided.	Specify why not: This is not a system of records

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: It is part of the business process to collect business contact related PII.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: It is part of the business process to collect business contact related PII.

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 OTEXA administrators to change/update business related 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.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	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: Audit log review for logins.
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): 11-04-2024 ☐ 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.
	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.

Section 9: Privacy Act

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

____ Yes, the PII/BII is searchable by a personal identifier.

_X__ 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."

	Yes, this system is covered by an existing system of records notice (SORN).
	Yes, a SORN has been submitted to the Department for approval on (date).
X	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.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule.
	Yes, retention is monitored for compliance to the schedule.
X	No, retention is not monitored for compliance to the schedule. Provide explanation: This is not a system of records.

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.)

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.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: There is very little PII contained in the system overall. All PII collected is non-sensitive PII related to business contact information.
X	Data Field Sensitivity	Provide explanation: The information collected is not particularly sensitive.
X	Context of Use	Provide explanation: All PII collected is non-sensitive PII related to business contact information.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The information is maintained in a secure system and accessed only by USG personnel for official use.
	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.)

For Commercial Availability, the amount of information requested has been reduced to the minimum necessary to determine whether or not the subject product is commercially available in a timely manner from suppliers in the United States.

All information is collected directly from account holders (Haiti), participants in a Commercial Availability proceeding, and/or companies listed in the Made in the USA Sourcing and Products Directory.

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.