U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
VASTEC Data Conversion System (DCS)

Reviewed by: David Chiles, 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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary,
cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.01.18 10:47:04 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO VASTEC Data Conversion System (DCS)

Unique Project Identifier: [2402] PTOC-012-00

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) a general description of the information in the system

The Virtual Accessible Sustainable Technology (VASTEC) Data Conversion System (DCS) has been implemented in support of the Continuous Data Conversion (CDC) and Backfile/Pre-1971 Patent Conversion projects. The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents to Extensible Markup Language (XML) documents based on a predefined XML schema. The files in the new XML format allow patent examiners to search, manage, and manipulate different document types, using examination tools under development.

VASTEC DCS receives a USPTO bundle of document files for batch process to the VASTEC DCS office through Secured File Transfer Protocol (SFTP). After the conversion is performed the output is returned to USPTO Patent Capture and Applications Processing System – Examination Support (PCAPS-ES) PATI-CDC in a VASTEC DCS bundle. A bundle is the basic unit of recovery point objective in case of failure. The recovery of interrupted processing starts with the last USPTO bundle received, if it is intact. Otherwise the USPTO bundle is retrieved from USPTO.

Key modules of the Data Conversion System include PrepPatent which performs file decompression, multipage TIFF creation, metadata lookup, and renaming. The ProcessPatent module executes high-speed automated file distribution, completes file transfer and ProcessPatent verifies file counts, page counts, and conversion stage success. Another key part of the solution is the PrimeOCR software. PrimeOCR converts multipage TIFF images to a PrimeOCR XML/Pro format. The system then converts the content of the PrimeOCR XML/Pro output to a customized USPTO XML (XML4IP) format.

The components of the VASTEC DCS Data Conversion System resides within an access restricted data center, leveraging security badge control, at the VASTEC DCS facilities in Tampa, FL.

(b) a description of a typical transaction conducted on the system

VASTEC DCS receives patent applications directly from the United States Patent and Trademark Office (USPTO).

(c) any information sharing conducted by the system

VASTEC DCS does not share any information with other agencies, individuals, or organizations. The information provided by USPTO is used by VASTEC DCS for authorized data conversion activities performed by internal personnel only.

(d) a citation of the legal authority to collect PII and/or BII

This PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. It is provided to VASTEC DCS so that data conversion activities can be performed on the collected patent application. The legal authority to collect PII and/or BII derives from 35 U.S.C. 1, 6, and 115; 5 U.S.C. 301 (SORN COMMERCE/PAT-TM-7).

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *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):					

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*	☐	e. File/Case ID	☒	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: NA					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: NA					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☐	i. Home Address	☐	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐

s.	Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	☒	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☒		
i. Other work-related data (specify): NA					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify): NA					

System Administration/Audit Data (SAAD)

a. User ID	☐	c. Date/Time of Access	☐	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify): NA					

Other Information (specify) DCS collects the information for up to 4 hours during conversion. No data is collected past the 4 hours.

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	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify): NA					

Government Sources

Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify): NA					

Non-government Sources

Public Organizations	☐	Private Sector	☒	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): NA					

2.3   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):			

☒	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):			

☒	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			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	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):			

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).

This PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. VASTEC DCS does not store any data after processing and it is directly transmitted back to USPTO. The PII/BII comes from persons applying for patents through the USPTO. This could include federal employees, contractors, members of the public, or foreign nationals.

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	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☒	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2   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:
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3   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	☐	Government Employees	☐
Contractors	☒		
Other (specify): VASTEC DCS employees working on data conversion and DCS authorized admins			

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:
☒	No, notice is not provided.	Specify why not: Specify why not: Individuals may be notified that their PII/BII is collected, maintained, or disseminated by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-7, Patent Application Files. That information is volunteered by individuals as a part of the patent application process.

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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals may have the opportunity to decline to provide their PII/BII. That option would be offered by the primary patent application ingress system, which is covered

		under the system of records at USPTO: COMMERCE/PAT-TM-7, Patent Application Files. That information is volunteered by individuals as a part of the patent application process.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals may have the opportunity to consent to particular uses of their PII/BII. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-7, Patent Application Files. That information is volunteered by individuals as a part of the patent application process.

7.4   Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Specify why not: Individuals may have the opportunity to review/update the PII/BII pertaining to them. That option would be offered by the primary patent application ingress system, which is covered under the system of records at USPTO: COMMERCE/PAT-TM-7, Patent Application Files. That information is volunteered by individuals as a part of the patent application process.

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.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to the information system is limited to system administrators only. Each administrator has a unique logon ID. All successful and unsuccessful logons to the system are recorded.

☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>March 6, 2017</u> ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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 (POAM).
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☐	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.

Access to the system and data are limited to system administrators and software developers. Data is received, processed, and returned. This is usually within four hours. All transfers of data between VASTEC DCS and USPTO occur over a FIPS 140-2 certified secure file transport system.

Section 9: Privacy Act

9.1   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). Provide the SORN name and number *(list all that apply)*:
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☒	No, a SORN is not being created. The system is covered under the following SORN already in existence. Patent Application Files—PAT/TM—7 http://www.uspto.gov/sites/default/files/sorn/uspto-pasorn-07.pdf

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: This is provided by the USPTO. http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/records_mgmt_crs.html. Patent Case Files, Granted [N1-241-10-1:2] Additional record control schedule information is available on NARA's website: http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-commerce/rg-0241.
☐	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:
☒	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	☐	Overwriting	☒

Degaussing	☐	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

☐	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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, title, address, phone number, email.
☒	Quantity of PII	Provide explanation: PII is only on the system for the time it takes to process and return to USPTO. This is usually less than four hours.
☐	Data Field Sensitivity	Provide explanation:
☒	Context of Use	Provide explanation: information is for identifying and tracking patent applicants/applications.
☐	Obligation to Protect Confidentiality	Provide explanation:
☒	Access to and Location of PII	Provide explanation: access is limited to VASTEC DCS staff on a closed system.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1   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:

☒	No, the conduct of this PIA does not result in any required business process changes.

12.2 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:
☒	No, the conduct of this PIA does not result in any required technology changes.