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

**Privacy Threshold Analysis
for the
VASTEC Data Conversion System (DCS)**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO VASTEC Data Conversion System (DCS)

Unique Project Identifier: PTOC-012-00

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: *Provide a brief description of the information system.*
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).

The 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 receives a USPTO bundle of document files for batch process in the Tampa VASTEC DCS through Secured File Transfer Protocol (SFTP). After the conversion is performed, the output is returned to USPTO in a VASTEC 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.

Address the following elements:

a) *Whether it is a general support system, major application, or other type of system*
VASTEC Data Conversion System (DCS) is a Major Application.

b) *System location*

VASTEC Data Conversion System (DCS) is located in Tampa, Florida.

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

VASTEC Data Conversion System (DCS) is an external contractor system that has been
implemented in support of the Continuous data Conversion (CDC).

d) The purpose that the system is designed to serve

The purpose of the system is to transform electronic Tagged Image File Format (TIFF) images of patent application documents into Extensible Markup Language (XML) documents based on a predefined XML schema.

e) The way the system operates to achieve the purpose

Data transfer between USPTO and DCS is done via a secure transport system. The transfers take place over public internet, from DCS to USPTO through their (USPTO) TIC (trusted Internet Connection).

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

The type of information collected, maintained, used, or disseminated by the system are patent
information.

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

Information provided by USPTO is used by DCS for authorized data conversion activities
performed by internal personnel only.

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

The files in the new XML format allow patent examiners to search, manage, and manipulate
different document types, using examination tools under development.

i) How information is transmitted to and from the system

VASTEC Data Conversion System (DCS) receives patent applications directly from the United States Patent and Trademark Office (USPTO). Data transfer between DCS and USPTO is done via a secure transport system. The transfers take place over public internet, from DCS to USPTO through their TIC (trusted internet connection).

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. *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.

☒ 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.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

    ☒   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.)."

    ☐   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."

    ☒   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
        ☐ 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.

☒   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?

☒   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.

☒   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

☒ The criteria implied by one or more of the questions above **apply** to the VASTEC Data Conversion System (DCS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the VASTEC Data Conversion System (DCS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner	**Chief Information Security Officer**
Name: Yang Nelson Office: Office of Information Technology (OITP) Phone: (571) 272-0826 Email: Nelson.Yang@uspto.gov Signature: _____ Date signed: _____	Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: _____ Date signed: _____
Privacy Act Officer	**Bureau Chief Privacy Officer and Co-Authorizing Official**
Name: John Heaton Office: Office of General Law (O/GL) Phone: (703) 756-1240 Email: Ricou.Heaton@uspto.gov Signature: John Ricou Heaton _Digitally signed by John Ricou Heaton Date: 2023.08.11 09:48:56 -04'00'_ Date signed: _____	Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: _____ Date signed: _____
Co-Authorizing Official	
Name: Vaishali Udupa Office: Office of the Commissioner for Patents Phone: (571) 272-8800 Email: Vaishali.Udupa@uspto.gov Signature: _____ Date signed: _____	