Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
Serco Patent Processing System (PPS)

Reviewed by: Henry J. Holcombe, 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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2021.06.23 06:59:49 -04'00' 05/12/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Serco Patent Processing System (PPS)

Unique Project Identifier: PTOC-016-00

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.

Serco Patent Processing System (PPS) is a Major Application (MA). This system processes electronic images of patent applications received by Serco Inc. from the United States Patent and Trademark Office (USPTO). Patent applications consist of electronic documents that conform to requirements as defined by USPTO. The system consists of a variety of application review tools, research tools, and data entry tools to facilitate the evaluation and classification of the application creating a series of U.S. Patent Classification (USPC) system and Cooperative Patent Classification (CPC) system classification data elements that describe the application. The PPS is dedicated to securely processing patent information. The system is physically located at the contractor staffed and operated facility located at Serco Inc., 1450 Technology Drive, Harrisonburg, VA 22802.

(a) Whether it is a general support system, major application, or other type of system
Serco PPS is a major application (MA) system.

(b) System location
The system is located in Harrisonburg, VA 22802

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
Serco PPS interconnects with the USPTO File Transfer System

(d) The way the system operates to achieve the purpose(s) identified in Section 4
Serco PPS processes inbound electronic images of patent applications provided by USPTO. The patent applications consist of electronic applications that conform to the application requirements. Applications need to contain all required sections and content to be deemed complete.

(e) How information in the system is retrieved by the user
Information is retrieved by user utilizing a toolset that consists of a variety of application review, research tools, and data entry tools to facilitate the evaluation and classification of the application creating a series of classification data elements that describe the application.

(f) How information is transmitted to and from the system
Serco PPS receives patent applications directly from the USPTO via secure channel. The PPS transport subsystem uses encryption to ensure secure transmission of sensitive data between USPTO and the Serco facility.

(g) Any information sharing conducted by the system
Serco PPS does not share any information with other agencies, individuals, or organizations. Serco uses the information provided by USPTO for authorized activities performed by authorized personnel only.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
35 U.S.C. 1, 2, and 115

(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-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.

☒ 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).

☐ 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	☒				
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	☒	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): Inventor Citizenship					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☒
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	☒	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	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify):					

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

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

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

Serco ensures accuracy of the information in the system by only allowing authorized users read access to content provided by USPTO. Users are not allowed to change the content provided by the USPTO. Additionally, Serco validates data elements returned to USPTO prior to submission. The transport subsystem consists of system components designed to support receipt of inbound patent applications from USPTO and for transmission of Serco deliverables back to USPTO. The PPS transport subsystem uses strong encryption to ensure secure transmission of sensitive data between USPTO and the Serco PPS.

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. 0651-0031 Patent Processing 0651-0032 Initial Patent Applications
☐	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):			

☒	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			
For a Computer Matching Program	☐	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).

The PII and/or BII data is collected by the USPTO to facilitate the patent application process. 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.

The information is part of the official record of the application and is used to document Inventor location and nationality and for communications.

During processing, the information is not shared with any entity outside of the Serco PPS, neither with other components of Serco, nor externally to any commercial business partners.

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.)

Foreign and adversarial entities as well as insider threats are the predominant threats to the information collected and its privacy. The system has implemented security controls following National Institute of Standards and Technology (NIST) guidance to deter and prevent threats to privacy.

Serco provides technical controls that are put in place to include; connections to the PPS infrastructure within the Serco facility are physically and logically controlled, Physical access to ports is restricted through the use of locks and a badge access system and Logical access to ports is controlled. All physical access to the server room is controlled by the badge activated access control system and only administrators and select individuals have clearance.

Serco provides annual training for system users regarding appropriate handling of information. During processing, the information is not shared with any entity outside of the Serco PPS, neither with other components of Serco, nor externally to any commercial business partners.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	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: Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII via file transfer. The technical controls that are put in place include; connections to the PPS infrastructure within the Serco facility are physically and logically controlled, Physical access to ports is restricted through the use of locks and a badge access system and Logical access to ports is controlled. All physical access to the server room is controlled by the badge activated access control system and only administrators and select

	individuals have clearance Serco Patent Processing System (PPS) connects to USPTO File Transfer system. According to 35 U.S.C. Section 122, USPTO must maintain patent applications in confidence. In order for Serco to support this, the PPS which processes unpublished patent application data have undergone a formal IT Security Certification & Accreditation process and have been approved for operation with the requisite and appropriate security controls in place and in conformance with Federal IT Security Policy. Specific safeguards that are employed by Serco PPS to protect the patent applications include: • The PPS system and its facility are physically isolated and closely monitored. Only individuals authorized by USPTO are allowed access to the system. • All patent information is encrypted when transferred between PPS and USPTO using secure electronic methods. • All patent information is encrypted before leaving the facility and is stored at backup facilities in encrypted form. • Technical, operational, and management security controls are in place at PPS and are verified regularly. • Periodic security testing is conducted on the PPS system to help assure than any new security vulnerabilities are discovered and fixed. • All PPS personnel are trained to securely handle patent information and to understand their responsibilities for protecting patents.
☐	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	☐	Government Employees	☐
Contractors	☒		
Other (specify): There are three general classes of users in the PPS environment which are; Managers, Users, and System Administrators. **Managers:** limited number of people who are able to assign, view work, approve work, and have been qualified and trained to define and manage the workflow through the application interfaces. They have administrator privileges in the workflow application, but they do not have system administrator privileges on servers or platforms. **General Users:** Are organized into groups based on their work assignment. At any given time, there are potentially up to 200 users when fully operational capabilities are utilized. Users are only able to see work assigned to their Group (Team Leads) or work assigned to them (Classifiers). Once the work leaves the work queue, it will no longer be visible in the work queue for that work task. **System Administrators:** Have full system administrator rights on servers and workstations, and can add/delete/modify user system rights, with consultation from the ISSO.			

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: https://www.uspto.gov/privacy-policy _____.	
☒	Yes, notice is provided by other means.	Specify how: Notice is provided at the time of collection by the Patent front end systems during initial application processing. 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.
☐	No, notice is not provided.	Specify why not:

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: 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. The PII/BII contained in this information is needed for successful processing of the patent application.
☐	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.

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: 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. The PII/BII contained in this information is needed for successful processing of the patent application.
☐	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.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: 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. The PII/BII contained in this information is needed for successful processing of the patent application.
☐	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.
☒	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: Implementation is tracked in the Serco PPS System Security Plan (SSP)
☒	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): ___6/11/2020_____ ☐ 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 (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.

☒	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.
☒	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).*

Access to the system and data are limited to classifiers, management, and system administrators. Data is received, processed through the Serco PPS workflow, and returned to USPTO. All transfers of data between Serco PPS and USPTO occur over a secure file transport system.

From an external standpoint, PPS processes inbound electronic images of patent applications. These applications consist of electronic images that conform to the patent application requirement by USPTO. The transport subsystem consists of system components designed to support receipt of inbound patent applications from USPTO and for transmission of Serco deliverables back to USPTO. The PPS transport subsystem uses strong encryption to ensure secure transmission of sensitive data between USPTO and the Serco PPS.

Once transferred to the Serco PPS, applications are processed by a custom developed Serco distributed computing engine. These applications are then passed through the workflow system where they are monitored throughout the entire process. Reports of these processes will be generated by the Workflow system. After each application has been properly classified by the System and Patent classifiers, the system will extract and encrypt metadata about the application and send these back to USPTO.

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.

☐ 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). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/PAT-TM-7 Patent Application Files Systems of Records.
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-10-1:10.3: Patent Administrative Feeder Records
☐	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 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.)*

☐	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: Name, title, address, phone number, email and citizenship status can be used to identify an individual.
☒	Quantity of PII	Provide explanation: PII is stored within the PPS application system and store large quantities of data that contains PII from the USPTO network.
☒	Data Field Sensitivity	Provide explanation: data includes limited personal and work related elements and does not include sensitive identifiable information
☒	Context of Use	Provide explanation: Information is for identifying and tracking patent applicants & applications.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the Privacy Act of 1974, PII must be protected and Serco utilizes identification and authentication as a technical measure to prevent unauthorized people (or unauthorized processes) from entering PPS IT system.
☒	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission.
☐	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.)

Foreign entities and adversarial entities including insider threats are the predominant threats to the information collected and its privacy. Security controls following NIST guidance are implemented to deter and prevent threats to privacy. Currently there are no known threats to privacy existent in light of the information collected from the USPTO.

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