

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



**Privacy Impact Assessment  
for the  
Information Delivery Product (IDP)**

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

- ☒ 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: 2018.09.14 16:23:07 -04'00'

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

Date

## **U.S. Department of Commerce Privacy Impact Assessment USPTO Information Delivery Product (IDP)**

**Unique Project Identifier: PTOC-003-00**

### **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*

Information Delivery Product (IDP) is a Master System composed of the following two (3) subsystems: 1) Enterprise Data Warehouse (EDW) , 2) Electronic Library for Financial Management System (EL4FMS) and 3) Financial Enterprise Data Management Tools (FEDMT)

#### **Enterprise Data Warehouse (EDW)**

The Enterprise Data Warehouse (EDW) system is an automated information system (AIS) that provides access to integrated United States Patent and Trademark Office (USPTO) data to support the decision-making activities of managers and analysts in the USPTO's business areas as needed to achieve business goals. It helps USPTO managers and analysts to answer a variety of strategic and tactical business questions using quantitative enterprise business information. Specifically, EDW provides a tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business.

The Enterprise Data Warehouse:

Provides an integrated view of PTO's business information about PTO General Ledger, Revenue, Payroll, Cost Accounting, Human Resources, Budget, Compensation Cost Projection, Patent Case, Patent Examiner Production, Time and Attendance, Federal Procurement, Corporate Planning, Contractor Actual, Fixed Assets, Automated Disbursements, Accounts Receivable, Travel, Accounts Payable, Acquisitions, IT Project Information, IT Deployment, and Patent Trial and Appeal Board (PTAB) data to support strategic and tactical decision-making. Enables business users to retrieve and analyze USPTO business information at their desktop without assistance from information technology specialists.

Supports analyses of USPTO data as necessary to supply parameter data, derived from actual historical information, needed by analytical models such as the Patent Resource Management System (PRMS) and the Corporate Planning Tool.

#### **Electronic Library for Financial Management System (EL4FMS)**

The Electronic Library for Financial Management Systems (EL4FMS) is an automated information system (AIS) that provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. EL4FMS also supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account.

**Financial Enterprise Data Management Tools (FEDMT)**

FEDMT is a database/user interface solution utilizing the Oracle APEX product to build small applications to support Financial Reference data.

The first usage of this application built the PPA Code Database project that developed an APEX database within the current OCFO ABIS system boundary to house PPA (Program, Project, and Activity) code data that currently resides in two standalone Microsoft Access databases, each separately maintained by OCIO FRMD and OCFO ABID. Both existing Access databases contain a complete listing of PPA codes; the differentiator is the OCIO database contains additional project-related attributes of interest to FRMD. The new APEX database serves the need of both OCFO and OCIO and contains additional attributes needed by FRMD.

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

A typical transaction is to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data necessary to supply parameter data derived from actual historical information needed by analytical models, such as OPBudget and the Corporate Planning Tool (CPT) to achieve USPTO's business information, a variety of strategic and tactical business questions. Specifically, the information will provide managers and analysts the ability to analyze business processes, resource use and needs, and other facts of the business at their desktop without assistance from information technology specialists. The information is collected to provide a single data source to facilitate ad-hoc queries and analysis of data by managers and analysts in the USPTO's business areas at their desktop without assistance from information technology specialists. Specifically, the system will provide a tool that enables managers and analysts to analyze business processes, resource use and needs, and other facets of the business and provide the USPTO with the means of performing at a more efficient, accurate, and cost effective level.

EL4FMS also supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account.

FEDMT builds small applications to support Financial Reference data.

*(c) any information sharing conducted by the system*

IDP does not share any personal information with any external agencies. The information provided by USPTO is used by IDP for authorized activities performed by internal personnel only.

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

The PII and BII data is collected by the USPTO internal systems and it is provided to the IDP to provide managers and analysts the ability to analyze business processes, resource use and needs, and other facets of the business. The legal authority to collect PII and/or BII derives from

- 5 U.S.C. 301 and 35 U.S.C.6
- 35 U.S.C 1,6 and 115; 5 U.S.C. 301
- 35 U.S.C.2 and 41 and 15. U.S.C. 1113
- 5 U.S.C. 301; 44 U.S.C. 3101; 5 U.S.C. 4101 et seq.; 5 U.S.C. 1302, 3302, E.O 10577,3 CRF

1954-1958 Comp.p.218, E.O.12107, 3 CFR 1978 Comp. p264; and Federal Personnel Manual

(e) the Federal Information Processing Standard (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.)
- ☒ This is an existing information system in which changes do not create new privacy risks. Continue to answer questions, and complete certification.

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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.)

<b>Identifying Numbers (IN)</b>					
a. Social Security*	<input checked="" type="checkbox"/>	e. File/Case ID	<input type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
<p>*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:</p> <p>IDP maintains Social Security Numbers (SSNs) of USPTO employees for human resources reporting purposes. The source systems from which it receives SSNs are the U.S Department of Agriculture (USDA) National Finance Center (NFC) and the USPTO Patent Capture and Application Processing</p>					

System – Examination Support (PCAPS-ES) Patent Application Location Monitoring (PALM) Infrastructure System (INFRA).

\*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:

The collection of SSNs could be avoided by using a different unique identifier for staff.

**General Personal Data (GPD)**

a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input checked="" type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input checked="" type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input checked="" type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input checked="" type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input checked="" type="checkbox"/>	l. Education	<input checked="" type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>

s. Other general personal data (specify):

**Work-Related Data (WRD)**

a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		

i. Other work-related data (specify):

**Distinguishing Features/Biometrics (DFB)**

a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>

j. Other distinguishing features/biometrics (specify):

**System Administration/Audit Data (SAAD)**

a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>

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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>				
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCBPNPD)</b>			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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.)*

<b>Activities</b>			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session )	<input type="checkbox"/>	For web measurement and customization technologies (multi-session )	<input type="checkbox"/>
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 Delivery Product integrates existing data from multiple USPTO sources and HR data from the U.S Department of Agriculture (USDA) National Finance Center (NFC). It makes data comparisons available for analysis.

This information is collected to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data. Specifically, the information will provide managers and analysts the ability to analyze business processes, resource use and needs, and other facets of the business and provide the USPTO with the means of performing at a more efficient, accurate, and cost effective level.

One subject area of the IDP is the Human Resources Subject Area (HRSA). HRSA is a reporting mechanism for HR to allow authorized users (both within OHR and for managers throughout PTO) to run reports, such as staff listings, within Grade Increases projections, employee counts, accession/separation lists, etc. The data warehouse (which stores USDA NFC, U.S Treasury HR Connect, and general employee locator content) in conjunction with the Business objects reporting tool, allows for the dissemination of information to authorized users.

### **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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>USPTO Systems:</p> <ul style="list-style-type: none"> <li>• Consolidated Financial System (CFS) <ul style="list-style-type: none"> <li>o Momentum</li> </ul> </li> <li>• Corporate Administrative Office System (CAOS) <ul style="list-style-type: none"> <li>o Web Time and Attendance (WebTA)</li> </ul> </li> <li>• Employee Relations/Labor Relations Case Management System (ERLRCMS)</li> <li>• Fee Processing Next Generation (FPNG)</li> <li>• Financial Budget and Planning System (FBPS) <ul style="list-style-type: none"> <li>o Corporate Planning Tool (CPT)</li> <li>o Financial Enterprise Data Management Tools (FEDMT)</li> <li>o Transit Subsidy System (TSS)</li> </ul> </li> <li>• Patent Capture and Application Processing System – Examination Support (PCAPS-ES) <ul style="list-style-type: none"> <li>o Patent Application Location Monitoring (PALM) Examination and Post-Examination (EXPO)</li> <li>o Patent Application Location Monitoring (PALM) Infrastructure System (INFRA)</li> </ul> </li> <li>• Patent Trial and Appeal Board End to End (PTAB E2E)</li> <li>• Reasonable Accommodation Case Management System (RACMS)</li> <li>• Revenue Account and Management (RAM)</li> </ul> <p>External Systems:</p> <ul style="list-style-type: none"> <li>• U.S. Department of Agriculture (USDA) National Finance Center (NFC)</li> <li>• U.S. Treasury HR Connect</li> </ul> <p>The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) and the Enterprise Monitoring and Security Operations (EMSO) systems.</p>
-------------------------------------	--



<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.*)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input type="checkbox"/>	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: _____.	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). Individuals may be notified that their PII/BII is collected, maintained, or disseminated by the primary application ingress system.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. IDP has no authorization to decline any type of information since it's owned by the primary applicat

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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: IDP receives PII/BII indirectly from application systems (i.e front end systems). These front end systems provide this functionality for data that is being collected.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Specify why not: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. IDP has no authorization to review/update any type of information since it's owned by the primary application.

## **Section 8: Administrative and Technological Controls**

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to the PII/BII is being monitored and tracked through audit logs.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/19/17 <input type="checkbox"/> This is a new system.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

## 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

### Management Controls:

The USPTO uses the Life Cycle review process to ensure that management controls are in place for the IDP. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational, and technical controls that are in place, and planned during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

### Operational Controls:

Operational controls include securing all hardware associated with this system in the USPTO Data Center. The Data Center is controlled by access card entry, and manned by a uniformed guard service to restrict access to the servers, their operation systems and databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions” (2) Physical terminal identification; (3) Database UserID; (4) restricted data display, as required; and (5) restricted access.

### Technical Controls:

Technical controls include password authentication (userid and passwords). At the client PCs’, access is managed through a password authentication (userid and passwords) based on certification on a Financial Application Security Registration form. The security form must be signed by a supervisor, and requires additional approval from Human Resources based on a justification of need.

## **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.”

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): Existing Systems Records cover the information pulled from other systems residing in the Enterprise Data Warehouse. These include:</p> <ul style="list-style-type: none"> <li>• Commerce/PAT-TM 3, Employee Production records;</li> <li>• Commerce/PAT-TM-7, Patent Application Files;</li> <li>• Commerce/PAT-TM 10, Patent Deposit Accounts System; and</li> <li>• Commerce/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.</li> </ul>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .

<input type="checkbox"/>	No, a SORN is not being created.
--------------------------	----------------------------------

## **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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: GRS 4.3:031 – Output Records
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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.)*

<b>Disposal</b>			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Social Security Number (SSN), name, gender, age, race/ethnicity, home/business address, email address, telephone number, financial information
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Collectively, the number of records maintained generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Combination of name, SSN, and financial information may be more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: PII is stored to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission
<input type="checkbox"/>	Other:	Provide explanation:

## **Section 12: Analysis**

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.