

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



**Privacy Impact Assessment  
for the  
USPTO AINS eCase SaaS System (UAECSS)**

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*

---

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

Date

## **U.S. Department of Commerce Privacy Impact Assessment USPTO USPTO AINS eCase SaaS System (UAECSS)**

**Unique Project Identifier: PTO-EBPL-LT-AINS eCase SaaS System (EBPL-LT-03-00)**

### **Introduction: System Description**

*Provide a brief description of the information system.*

The CSP AINS eCase SaaS Solutions Platform (UAECSS) is a commercial SaaS (Software as a Service) implemented with AINS eCase/FOIAxpress. This SaaS provides for end-to-end processing of Freedom of Information Act (FOIA) and Privacy Act requests and appeals. The system electronically stores, retrieves, and redacts documents for delivery to requesters. UAECSS offers multiple applications, however USPTO's Office of General Counsel (OGC) requires only the FOIAxpress (FX) application to facilitate the capability to process FOIA requests, support FOIA case management workflow processes, tracking and reporting a wide range of USPTO FOIA processes.

Address the following elements:

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

The USPTO-AINS eCase System (UAECSS) is a Software as a Service (SaaS)..

*(b) System location*

UAECSS is cloud FedRAMP Authorized SaaS located in Equinix data center in Gaithersburg, MD.

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

UAECSS interconnects with the following systems:

**ESS** – Enterprise Software Services (ESS) The Enterprise Software Services (ESS) system ESS is comprised of multiple on premise and in the cloud software services which support the USPTO in carrying out its daily tasks. ESS provides an architecture capable supporting current software services as well as provide the necessary architecture to support the growth anticipated over the next five years

**NSI** - Network and Security Infrastructure System (NSI) is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access,

protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

**DBS** – Database Services (DBS) is an Infrastructure information system, and provides a Database Infrastructure to support the mission of USPTO database needs.

**EWS** – Enterprise Windows Servers (EWS) is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

**EUS** - Enterprise Unix Services (EUS) consists of assorted UNIX operating system variants (OS), each comprised of many utilities along with the master control program, the kernel.

*(d) The way the system operates to achieve the purpose(s) identified in Section 4*

The UAECSS system provides a workflow that tracks and facilitates the processing of FOIA and Privacy Act requests. The system provides a correspondence capability to communicate with requesters and program offices. The system has a document management capability to store, retrieve, redact, and produce document releases.

*(e) How information in the system is retrieved by the user*

UAECSS is a web application that allows authorized users to access and view information in the system using a web browser.

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

UAECSS users use a web browser to make a Hypertext Transfer Protocol Secure (HTTPS) connection to web application; the system also uses Simple Mail Transfer Protocol (SMTP) to send email correspondence.

*(g) Any information sharing*

UAECSS does not share information.

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

Freedom of Information Act, 5 U.S.C. 552; Privacy Act of 1974 as amended, 5 U.S.C. 552a; 5 U.S.C. 301, and 44 U.S.C. 3101.

*(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.)*

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

## **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"/>	f. Driver's License	<input checked="" type="checkbox"/>	j. Financial Account
b. Taxpayer ID	<input checked="" type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction
c. Employer ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>	m. Medical Record
e. File/Case ID	<input checked="" type="checkbox"/>			
n. Other identifying numbers (specify):				
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: PII/BII may be incidentally collected and maintained as a result from FOIA or Privacy Act search requests of agency record but such content is redacted before sending to the requester.				

<b>General Personal Data (GPD)</b>				
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input checked="" type="checkbox"/>	o. Financial Information
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input checked="" type="checkbox"/>	p. Medical Information
c. Alias	<input checked="" type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service
d. Gender	<input checked="" type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record
e. Age	<input checked="" type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status
f. Race/Ethnicity	<input checked="" type="checkbox"/>	m. Education	<input checked="" type="checkbox"/>	t. Mother's Maiden Name

g. Citizenship	<input checked="" type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify): PII/BII may be incidentally collected and maintained as a result from FOIA or Privacy Act search requests of agency records.					

<b>Work-Related Data (WRD)</b>					
a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input checked="" type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input checked="" type="checkbox"/>	k. Procurement/contracting records	<input checked="" type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input checked="" type="checkbox"/>		
l. Other work-related data (specify): PII/BII may be incidentally collected and maintained as a result from FOIA or Privacy Act search requests of agency records.					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input checked="" type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. UserID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	f. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					
PII/BII may be incidentally collected and maintained as a result from FOIA or Privacy Act search requests of agency records. This content is redacted before sending to the requester and exempt from disclosure, except in cases where the PII/BII belongs to the individual requester of a Privacy Act request.					

2.2 Indicate sources of the PII/BII in the system. (*Check all that apply.*)

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" 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 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 Describe how the accuracy of the information in the system is ensured.

<p>From an administrative perspective, the UAECSS application has administrative and support staff that function as points of contact for customers. USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and received by authorized users alone. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, the Perimeter Network (NSI) and EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities.</p>	
--	--

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	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.)*

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</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.)*

<b>Purpose</b>			
For a Computer Matching Program	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input checked="" 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 checked="" 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 PII/BII in the system is in reference to members of the public, PTO employees and contractors. The individual FOIA/PA requester (name, address, email, and phone) is used for the purpose of corresponding with the requester. During the course of a FOIA/PA request search, PII/BII may be incidentally collected from agency records. PII/BII is digitally redacted, manually redacted, withheld, and/or deleted. The information collected from agency records (as part of the FOIA/PA requests) may be judiciously disseminated as required by law. General routine uses are defined in the System of Records Notice [COMMERCE/DEPT-5](#) for Freedom of Information Act and Privacy Act Request Records. The system encompasses all individuals (public, federal employee/contractor, etc.) who submit FOIA and Privacy Act requests.

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 entities, adversarial entities and insider threats are the threats to privacy within this system. Inadvertent private information exposure is a risk and USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. USPTO requires Annual Security Awareness Training for all employees as well as policies and procedures documented in the Cybersecurity Baseline Policy. All USPTO offices adhere to USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

## **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 type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input checked="" 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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<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> <ul style="list-style-type: none"> <li>Enterprise Software Services (ESS) is comprised of multiple on-premise and in the cloud software services which support the USPTO in carrying out its daily tasks.</li> </ul> <p>The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved authorized accounts. USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO Cyber security personnel review audit logs received on a regular basis and alert the Information System Security Officer (ISSO) and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a “need to know” basis. Active Directory security groups are utilized to segregate users in accordance with their job functions.</p> <p>USPTO relies on FedRAMP Authorized AINS eCase SaaS, located in Equinix data center, to manage the cloud infrastructure including the network, data storage, system resources, data centers, security, reliability, and supporting hardware and software.</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.

6.4 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	<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 checked="" 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: <a href="http://www.uspto.gov/privacy-policy">http://www.uspto.gov/privacy-policy</a> .	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: Please see Appendix A: Privacy Act Statement
<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 checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals do not need to provide an address if correspondence is done via email. Individuals do not need to provide an email address if correspondence is done via postal mail. Individuals need to provide sufficient information to identify themselves for a Privacy Act request and to be able to receive correspondence.
<input type="checkbox"/>	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.

<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: Individuals who seek records from this system of records pertaining to themselves, must submit a request conforming with the Department's Privacy Act regulations set forth in 15 CFR part 4. Individuals must first verify their identities, meaning that they must provide their full name, current address and date and place of birth. Individuals must sign the request, and their signatures must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under perjury as a substitute for notarization.

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: USPTO employees and contractors have the opportunity to review and update their personal information online through NFC's Employee Personal Page application or the Department of Treasury's HR Connect system. Employees may also visit the USPTO's Office of Human Resources (OHR) department for additional assistance. These updates will change the information within Active Directory to update the users access privileges.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The requesters do not have the opportunity to update their PII within the system but they can request that their information be updated via email or mail.

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

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

<input checked="" 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: Audit Logs
<input checked="" type="checkbox"/>	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): 10/25/21 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<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 (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<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 DOC 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. (*Include data encryption in transit and/or at rest, if applicable.*)

Documents are reviewed for PII/BII and content is redacted before making it available to the individual requesters. The system implements encryption (SSL) for data at rest and in transit and authorized users are verified via role-based permissions.

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

A Security Categorization compliant with the FIPS 199 and NIST SP 800-60 requirements was conducted for UAECSS and this informs the security controls applied to the system.

## **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.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply)</i> :  <a href="#">COMMERCE / DEPT-5</a> Freedom of Information Act and Privacy Act Request Records
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:  <a href="#">GRS 4.2: Information Access and Protection Records</a>  Items 001: FOIA, Privacy Act, and classified documents administrative records Items 010: General information request files.
-------------------------------------	---

	Item 020: Access and disclosure request files Item 040: Records of accounting for and controlling access to records requested under FOIA, PA, and MDR Item 050: Privacy Act accounting of disclosure files Item 065: Privacy complaint files. Item 090: Privacy Act amendment request files
<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 type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.*)

<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 checked="" 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 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 level. (*Check all that apply.*)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: UAECSS collects, maintains, or disseminates PII about DOC employees and contractors. The types of information collected, maintained, used or disseminated by the system include name, address, email, and phone. When combined, this data set can be used to identify a particular individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The quantity is limited to the amount and type of requests received by the business unit and is moderate. A

		serious or substantial number of individuals would be affected by loss, theft, or compromise.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The combination of name, home address, telephone number, and email address do not make the data fields any more sensitive because they are publicly available information.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Data includes name and personal and work name, telephone number and email address as well as user ID and date/time access for purposes of FOIA and Privacy Act requests.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: UAECSS is a web application that allows authorized users to access and view information in the system using a web browser. Access is limited to authorized personnel only, government personnel, and contractors.
<input type="checkbox"/>	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.)

In addition to insider threats, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII in the form of personal and work-related data such as name, telephone number and email address as well as user ID and date/time access. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

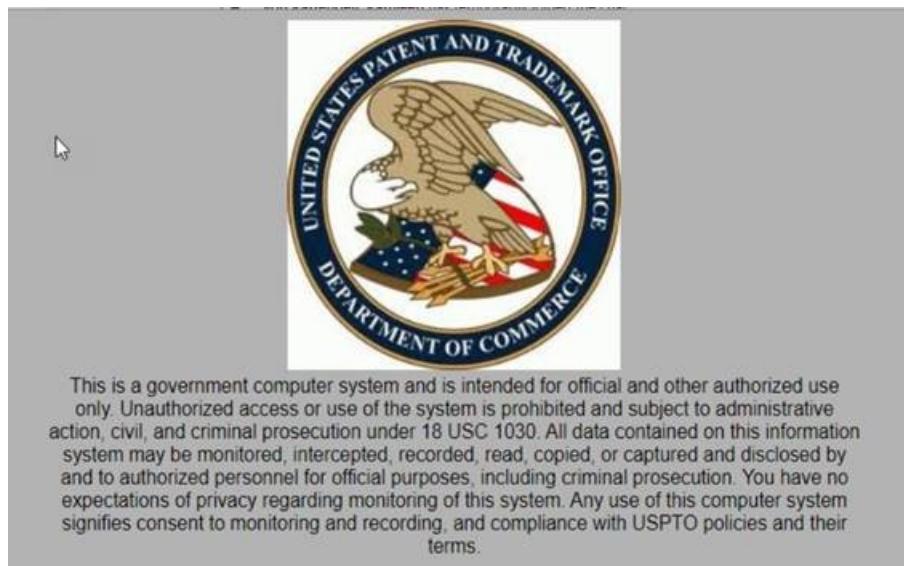
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<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.

12.3 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.

## Attachment A



This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.