Template Version Number: 01-2021

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

Users, Stephens, Deborah Digitally signed by Users, Stephens, Deborah
Date: 2023.01.30 12:25:36 -05'00'

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

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

Unique Project Identifier: EBPL-LT-03-00

Introduction: System Description

Provide a brief description of the information system.

The USPTO AINS eCase SaaS Solutions Platform (UAECSS) is a commercial Software as a Service (SaaS) 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
UAECSS is a SaaS.

(b) System location
UAECSS is cloud FedRAMP Authorized SaaS located in Maryland, USA.

(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) system 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 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 (OS) variants, 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 applications; the system also uses Simple Mail Transfer Protocol (SMTP) to send email correspondence.

(g) Any information sharing
- UAECSS does not share information, the FOIA office uses the system to share information with the public in response to FOIA and PA requests.

.

(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.)*

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.

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. Marital Status	☐
f. Race/Ethnicity	☒	m. Education	☒	t. Mother's Maiden Name	☐

g. Citizenship	☒	n. Religion	☐		
u. Other general personal data (specify):					

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)
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.)*

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.

From an administrative perspective, the UAECSS application has administrative and support staff that function as points of contact for customers whereby customers may directly contact the administration for information accuracy. USPTO and CSP implement 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.

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.
☒	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): Click or tap here to enter text.			

☒	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/BII in the system is in reference to members of the public, PTO employees and contractors. They first need to have an account created in the application that includes their PTOnet Login Id. They can then use Okta SAML SSO to login to the application. 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 offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authorities or citations.

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: • ESS 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 bases 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. 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.
☐	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):			

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: Please see Appendix A: Privacy Act Statement
☐	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 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.
☒	No, individuals do not have an opportunity to decline to provide 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 37 CFR Subpart B.

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

☐	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Accounting logs are regularly requested by the public under the FOIA and are required to be provided with limited exceptions.

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: 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.
☒	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.)*

☒	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:
☒	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): 5/5/22 ☐ 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).*

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."

☒	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 / DEPT-5 Freedom of Information Act and Privacy Act Request 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: GRS 4.2: Information Access and Protection Records 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

☐	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: 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.
☒	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.
☒	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.
☒	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.
☒	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.
☒	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.
☐	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.

☐	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.

Attachment A