

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



**Privacy Impact Assessment
for the
Office of Enrollment and Discipline Item Bank – Cloud (OEDIB-C)**

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2023.02.10 15:47:07 -05'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Office of Enrollment and Discipline Item Bank – Cloud (OEDIB-C)

Unique Project Identifier: EBPL-LT-04-00

Introduction: System Description

Provide a brief description of the information system.

Office of Enrollment and Discipline Item Bank – Cloud (OEDIB-C) (commercial name Questionmark OnDemand for Government) is a Federal Risk and Authorization Management Program (FedRAMP) authorized Software as a Service (SaaS). OEDIB-C is used by the Office of Enrollment and Discipline (OED) staff to develop and maintain exam content for the Attorney and Agent Registration Exams.

Address the following elements:

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

Office of Enrollment and Discipline Item Bank – Cloud (OEDIB-C) is a minor application.

(b) System location

OEDIB-C is hosted in a FedRAMP certified Microsoft Azure Government Cloud in Virginia.

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

OEDIB-C interconnects with the following systems:

- **Identity and Credential Access Management (ICAM-IDaaS)-Identity as a Service (IDaaS):** ICAM-IDaaS provides authentication and authorization services to USPTO applications.

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

The system is accessed through a web application with an updatable item repository, test creation capability, test delivery, and a report generator for OED users. OED users log-in to OEDIB-C using ICAM-IDaaS single sign-on and will navigate through OEDIB-C to develop and maintain exam content and assessments for the Attorney and Agent Registration exams.

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

OEDIB-C 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

OEDIB-C users use a web browser to make a Hypertext Transfer Protocol Secure (HTTPS) connection to the web application.

(g) Any information sharing

The OED business exports exam content from OEDIB-C and provides it to Prometric for them to offer the exam to registration applicants.

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

35 USC 2(b)(2)(D)

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

OEDIB-C is a Moderate FIPS categorized system.

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	<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):					

☐ 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*	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>

b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input type="checkbox"/>				
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	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input checked="" type="checkbox"/>
c. Work Address	<input type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input 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):					

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

Government Sources					
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):					

Non-government Sources					
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>The user accounts, which contain the user's name and email address, are created in the OEDIB-C system when the user first authenticates using ICAM-IDaaS. This information comes directly from Active Directory (AD) as an accurate and authoritative source.</p> <p>The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.</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.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
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.)

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify): Click or tap here to enter text.			

<input checked="" type="checkbox"/>	There are not any IT systems 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	<input type="checkbox"/>	For administering human resources programs	<input 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 checked="" 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): To ensure the integrity of the proprietary Registration exam content, which is required to provide assessments that applicants must pass in order to become registered practitioners.			

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 proprietary Registration exam content is developed and maintained to provide assessments that applicants must pass in order to become registered practitioners. The exam content is provided to Commercial entity delivering the exam (currently Prometric via secure File Transfer Protocol (FTP)) in order for them to offer the exam to applicants in their nationwide testing centers. Applicants information is not collected, maintained or disseminated within OEDIB-C.

The name and work e-mail address are collected/maintained for federal employees and contractors for access to OEDIB-C. Their information is used within the system only for logging into OEDIB-C and for administrative purposes within the system.

- 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.)

The system maintains proprietary exam content that OED needs to protect in order to ensure exam integrity. Only authorized users and system administrators have access to OEDIB-C. OEDIB-C has implemented encryption for data in transit and data at rest. Authentication to the OEDIB-C application is managed using the Okta SAML Single Sign-On (SSO), which is multi-factor authentication.

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the 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 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 checked="" type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input 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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>ICAM-IDaaS</p> <p>NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices adhere to the USPTO Records Management Office's Comprehensive Records Schedule or the General Records Schedule and the corresponding disposition authority or citation.</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: https://www.uspto.gov/privacy-policy	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: See Appendix A
<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: The BII that is maintained and disseminated does not contain information regarding any individuals. The PII is related to the OEDIB-C users (employees and contractors) and administrators and is required for ensuring the integrity of the system. USPTO would not be able to ensure the protection of the BII without the collection of the PII.

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: The BII that is maintained and disseminated does not contain information regarding any individuals. The PII is related to the OEDIB-C users and administrators and is required for ensuring the integrity of the system. USPTO would not be able to ensure the protection of the BII without the collection of the PII.

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: The user's cannot update their information directly in OEDIB-C because the users' PII is obtained from ICAM IDaaS. System administrators can also be contacted to review/update PII pertaining to individuals.

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): <input checked="" 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 checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input checked="" 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest via Transport Layer Security (TLS) 1.2.

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> COMMERCE/DEPT-25 Access Control and Identity Management System PAT-TM-17 USPTO Security Access Control and Certificate Systems
<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: N1-241-09-1: b4.1 - Enrollment Examination
<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.)*

Disposal			
Shredding	<input type="checkbox"/>	Overwriting	<input checked="" 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: OEDIB-C collects and maintains PII about DOC employees and contractors. The types of information collected and maintained by the system include the user's name and work email address and could be used to identify an individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Since there are only 10 users of the OEDIB-C system, the quantity of PII is minimal.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Data fields include name and work email address which are not sensitive data points.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: OEDIB-C contains PII regarding users that need to be identified in a system they use to develop and manage exam content for the Attorney and Agent Registration Exams.
<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 with the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Role-based access restricts access to USPTO employees and contractors. All data are stored in FedRAMP-approved US Data Centers/Cloud locations.
<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.)

The scope of potential threat to privacy includes internal USPTO employees (insider threats) and OEDIB-C privileged users. Management controls are utilized by Questionmark and USPTO to prevent the inappropriate disclosure of sensitive information including Annual Security Awareness Training, which is mandatory for all Questionmark and USPTO employees. It includes training modules on understanding privacy responsibilities and procedures and other information such as defining PII and how it should be protected.

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

- 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.

Appendix 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.