Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
HireVue Recruitment Assessments and Video Interviewing (HireVue)

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER Date: 2026.08.07 11:17:54 -04'00' 8/6/2026

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO HireVue Recruitment Assessments and Video Interviewing (HireVue)

Unique Project Identifier: EBPL-PM-05-00

Introduction: System Description

Provide a brief description of the information system.

HireVue – Recruitment Assessment and Video Interviewing system is a cloud-based Software as a Service (SaaS) digital interviewing platform. The service provides the capability of online on-demand interviewing with ratings, recommendations and analytics for the purpose of aiding in the recruitment, assessing and hiring of qualified candidates for some positions at the United States Patent and Trademark Office (USPTO). The HireVue SaaS is Federal Risk and Authorization Management Program (FedRAMP) authorized with a FedRAMP Moderate impact level. HireVue is hosted in a government cloud (Amazon Web Service (AWS)) and interconnects with USPTO Okta authentication for SSO (single sign on) capability and Office 365 for Outlook Calendar integration.

Address the following elements:

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

HireVue is a general support system SaaS.

(b) System location

HireVue is hosted in AWS GovCloud environment, Alexandria, VA.

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

HireVue is interconnected to:

ICAM Identity as a Service (ICAM-IDaaS) - provides an enterprise authentication and authorization service to all applications/AIS's. ICAM-IDaaS is used to provide single sign-on capabilities for HireVue.

Ext365-Collaborative O365 (EUS)- provides integration with Microsoft Office 365 (MO 365) which is a line of subscription services offered by Microsoft as part of the Microsoft

Office product line. HireVue integrates with Microsoft Office 365 for calendar/scheduling functionalities.

Network and Security Infrastructure (NSI) – facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

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

HireVue is a cloud-based video interviewing platform that allows candidates to record on-demand interviews. USPTO hiring managers can log-in to view and evaluate recorded interviews at their convenience. Interviews are recorded and stored in the cloud environment for future reference. Once a job announcement closes, the office reviews applications to determine which candidates are the most qualified. These candidates will be placed on the certification (cert) list and are manually uploaded into HireVue by an administrator using the cert list with the candidate's first name, last name, and email address. After candidates are uploaded, each candidate is sent a system-generated email from HireVue with links to access the system.

Candidates can access their interview page and conduct their interview at their convenience within the allotted time. For these on-demand interviews, candidates record their interviews using their desktop/laptop webcam or smart-phone video camera. The candidates provide answers to structured, consistent, job-relevant questions or competency-based questions (which are preloaded into the system) without the presence of a recruiter or hiring manager.

For each position, questions can be created from scratch or pre-loaded questions covering various competencies can be selected using HireVue Builder saving time and providing a fairer and more structured interview process. Since the on-demand interviews are recorded, they can be accessed by recruiters or hiring manager for evaluation at their convenience. A candidate can be rated by one or more evaluators. Candidate responses to each question are rated and the evaluator(s) records a final recommendation for the candidate. Finally, the hiring coordinator(s) review the ratings and recommendations in HireVue to make a determination to hire a candidate and close out the record within the system. Anytime during this process, administrators are provided with analytics regarding candidates, ratings, and recommendations which can be downloaded as reports.

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

Users (USPTO designated staff and contractors) will have HireVue accounts and will log into HireVue to be able to access recorded interviews, and perform evaluations. Contractors will only have access for administrative purposes and will not have an active role in the

hiring process. Candidates are invited via email to provide information into HireVue; however, they are not defined as users within the system.

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

This is a cloud based online platform that will be available to the public (candidates) and designated USPTO employees for recorded on-demand video interviews. Information is transmitted via the internet using Hypertext Transfer Protocol Secure (HTTPS) (port 443) and via a connection to USPTO network. HireVue uses browser-based connections via HTTPS using Transport Layer Security (TLS) 1.2 encryption to application components.

(g) Any information sharing

Data collected will only be available to designate USPTO staff. The data will only be shared on a case-by-case basis with other DOC agencies, federal agencies, and the public.

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

Civil Service Reform Act of 1978, (October 13, 1978, Pub. L. 95–454, 92 Stat. 1111) (CSRA); 5 U.S. Code Subpart B - Employment and Retention; 5 C.F.R. Part 330, 337, 338, 35 U.S.C. 2.

(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): Interview Code					
*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. Sex	☐	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): Work related information such as occupation, job title, work history and previous employment performance ratings will not be explicitly requested however candidates may voluntarily provide this information during the interview process. Interview performance information will be collected and stored within HireVue.

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): Other distinguishing features such as hair color and are only captured via the video recording during the interview process. There is no other capturing of this information.

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☐
b. IP Address	☒	f. Queries Run	☐	f. Contents of Files	☐

g. Other system administration/audit data (specify):

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☒		

Other (specify):

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

Other (specify):

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐

Third Party Website or Application	☐		
Other (specify):			

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

The accuracy of the information in the system is ensured by obtaining the information directly from the individual from their application. 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.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0042 Patent Examiner Employment Application
☐	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): Video/audio recordings			

☐	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).

PII information consisting of public individuals name, e-mail, video and voice are to be used for interviewing, evaluating and interacting with USPTO employment candidates. Candidates will provide contact information (name and e-mail) and consent to asynchronous (recorded) interviews as part of the hiring process. Candidates will not be asked to provide other PII (general personal data and work-related data) but may voluntarily provide other PII information as a part of their recorded interview response. Designated USPTO staff and contractors will be granted accounts in HireVue to access recorded interviews, and perform assessments, and evaluations. In addition, USPTO staff and contractors will be able to construct interview questions, and generally control the interview process. Only USPTO staff name and email address are captured in HireVue.

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.)

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 of the USPTO adhere to the 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	☒	☐	☒
DOC bureaus	☒	☐	☐
Federal agencies	☒	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☒	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify): employment candidates	☒	☐	☐

☐	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: ICAM-IDaaS EUS NSI 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 of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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://hirevue.com/terms/	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as notice. . Notice is provided in the Terms and Conditions page displayed before candidates record the on-demand interview. The Terms and Conditions page contains a link to HireVue Privacy Policy and is displayed before any interview activity can proceed and requires agree or do not agree. If a candidate chooses "I do not agree" the HireVue system will end, and the candidate will be able to contact the USPTO point of contact to discuss other options. The following is a portion of what is displayed: Privacy Policy; Additional Terms 1. Privacy Policy. Please read the HireVue Privacy Policy https://www.hirevue.com/legal/privacy carefully for information relating to our collection, use, storage and disclosure of your personal information, and which is

		hereby incorporated by reference into, and made a part of, these Terms.
☐	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: Declining to provide the PII by choosing "I do not agree" to the Terms and Conditions page displayed before any interview activity takes place will be declining the Video interview and Candidates can then contact USPTO Point of Contact (POC) for other options.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: USPTO employees' name and work e-mail are required to access the system.

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: The system only collects and uses PII that is necessary to conduct the candidate interview, evaluation and rating. Candidates will be able to consent to use Video interviewing or Contact USPTO for other options.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The collection of the PII and BII is part of an interview process and is not designed for the candidate to be able to go back and edit their input. The name and contact information are obtained from the original application, if that information was incorrect the candidate would have to go back through the application process to get it updated. USPTO employees' name and work e-mail are required for access and are modified outside of this system.

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: Audit Logs
☒	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): 12/4/2025 ☐ 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 5 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).*

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.

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)*: OPM/GOVT 5: Recruiting, Examining and Placement 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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: Job Applicant Reports (N1-241-05-1:4e) Job vacancy case files (GRS 2.1:050) Job application packages (GRS 2.1:060) GRS 2.1: Employee Acquisition Records Item- 090 Interview records. GRS 3.1: General Technology Management Records Item - 020 Information technology operations and maintenance records. Which include access and audit logs. GRS 3.2. Information Systems Security Records, Item 010, 020, 040, 050 Which includes security logs.
☐	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: HireVue collects, maintains, or disseminates PII about USPTO employees, contractors, and the public. The types of information collected, maintained, used or disseminated by the system includes, first and last name, e-mail, interview code, likeness and voice, can be used to identify an individual.
☒	Quantity of PII	Provide explanation: The number of records collected generally is a significant amount of PII. There are approximately 15,000 candidates per year, with over 1,000 applications processed per month.
☒	Data Field Sensitivity	Provide explanation: The email address, first name, last name together can identify a particular person especially if the audio and/or video records are also available. This information together with the scores of the candidates can be sensitive as a part of the hiring process.
☒	Context of Use	Provide explanation: Designated USPTO staff will be granted accounts in HireVue to access recorded interviews and perform assessments and evaluations.
☒	Obligation to Protect Confidentiality	Provide explanation: In accordance with the Privacy Act of 1974, USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP

		800-122 and NIST SP 800-53 Rev5, Guide to Protecting the Confidentiality of Personally Identifiable Information.
☒	Access to and Location of PII	Provide explanation: Data will be stored within the AWS GovCloud environment.
☐	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 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.

☐	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.