Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
HireVue - Recruitment Assessments and Video Interviewing

U.S. Department of Commerce Privacy Threshold Analysis

USPTO HireVue - Recruitment Assessments and Video Interviewing

Unique Project Identifier: PPL-PBMI-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

HireVue – Recruitment Assessment and Video Interviewing system (HireVue) 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 USPTO. HireVue will initially be used by the Patents Business Unit for the recruitment and hiring of entry level examiners with the possibility of expansion to other business units in future years. The HireVue SaaS is FedRAMP authorized with a FedRAMP Moderate impact level. HireVue is hosted in a government cloud (Amazon Web Service (AWS)), and does not have interconnections by default but has been optionally configured to integrate with customer identity provider for single sign on and calendar integration to provide interview scheduling.

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.

b) *System location*

HireVue is hosted in AWS GovCloud environment.

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 USPTO employees and contractors for HireVue.

Microsoft Office 365 (MO 365) - A line of subscription services offered by Microsoft as part of the Microsoft Office product line. HireVue will integrate with Microsoft Office 365 for calendar/scheduling functionalities.

d) The purpose that the system is designed to serve

The purpose of the system is to provide a method by which the HR department can conduct candidate recorded interviews of employment candidates. Additionally, the purpose is to reduce the administrative burden of hiring officials, reduce hiring time, reduce cost and increase the efficiency in the hiring process of examiners, and non-examiners by conducting first round interviews using a 508 and FedRAMP compliant cloud-based SaaS digital interviewing platform.

e) *The way the system operates to achieve the purpose*

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 cert list and are manually uploaded into HireVue by an admin 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 by 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

HireVue includes PII collected, maintained, used or disseminated about employees, contractors, and members of the public. PII about employees, and contractors could include information such as work e-mail address and other work-related data. Information collected about members of the public, for hiring purposes, could include their first and last name, e-mail address and any additional personal information the candidate/member of the public voluntarily provides during the video and/or voice recordings.

Information collected, maintained, used or disseminated: first name, last name, e-mail address, video recording, voice recording.

g) Identify individuals who have access to information on the system

Designated individuals in USPTO Patents and HR Staff. The data will only be shared on a case by case basis with other DOC agencies, federal agencies and the public.

h) 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 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 E-Mail to provide information into HireVue. However, they are not defined as users within the system. Depending on the position the candidate submits the application for, they may or may not be able to go back into the system.

i) 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 HTTPS (port 443) and via a connection to USPTO network. HireVue uses browser-based connections via HTTPS using TLS 1.2 encryption to application components.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☒ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☒	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): The system records video of candidate interviews. Likeness and voice are captured.			

☐ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the ITsystem's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the HireVue - Recruitment Assessments and Video Interviewing and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the HireVue - Recruitment Assessments and Video Interviewing and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Peter (Toby) Brown Office: Office of Patent Administration (P/OPA) Phone: (571) 273-8030 Email: Petertoby.Brown@uspto.gov Signature: Users, Brown, Peter Toby Digitally signed by Users, Brown, Peter Toby Date: 2022.11.28 08:54:13 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2022.11.30 12:30:12 -05'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.11.29 13:05:02 -05'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2022.11.30 15:25:37 -05'00' Date signed: _____
Co-Authorizing Official Name: Andrew Faile Office: Office of the Commissioner for Patents Phone: (571) 272-8800 Email: Andrew.Faile@uspto.gov Signature: Users, Faile, Andrew Digitally signed by Users, Faile, Andrew Date: 2022.11.30 15:42:38 -05'00' Date signed: _____	