Privacy Impact Assessment for the VA IT System called:

HireVue -e

Veterans Benefits Administration

Human Capital Services

eMASS ID #: 2505

Date PIA submitted for review:

7/17/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	(909) 528-4958
Information System Owner	Chino Walters	chino.walters@va.gov	202-461-0452

Abstract

The abstract provides the simplest explanation for "what does the system do?".

HireVue will provide online interview capability for both on-demand and live interviews that is autonomous from or integrated with any Applicant Tracking System. It will also provide applicant access to on-Demand and live interviews. The SaaS will expedite and facilitate the interviewing and hiring of personnel, specifically in fulfilling the VA's mission "to care for him who shall have borne the battle, and for his widow, and his orphan" by serving and honoring the men and women who are America's Veterans. This includes estimated five (5) million Veterans and Servicemembers supported by the Promise to Address Comprehensive Toxics (PACT) Act.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

HireVue system will be controlled by the VBA Office of Human Capital Services.

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

VBA has a requirement for additional staff acquisition services so it can more effectively accomplish its mission. To achieve its important mission, VBA must retain the capacity to recruit and select a talented and motivated workforce. VBA needs a partner for staff acquisition support across numerous component groups who is uniquely positioned to provide the needed staffing support to VBA. The anticipated business impact of deploying this SaaS product is:

1) onboard VBA personnel, in support of the PACT Act and Veterans
2) reduce the administrative burden of hiring officials
3) reduce hiring time and cost
4) increase the efficiency in the hiring process

C. *Who is the owner or control of the IT system or project?*

VA Controlled / non-VA Owned and Operated.

2. *Information Collection and Sharing*

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

VBA is not able to provide an estimated number of users as this is a new system. The system will be used as a tool by both VBA hiring managers and applicants to automate the interview process.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

HireVue will provide online interview capability for both on-demand and live interviews that is autonomous from or can be integrated with any applicant tracking system. The system will expedite and facilitate the interviewing and hiring of personnel, specifically in fulfilling the VA's mission "to care for him who shall have borne the battle, and for his widow, and his orphan" by serving and honoring the men and women who are America's Veterans. HireVue is 508 compliant to meet Human Capital Services' usability, durability, storage, privacy and security requirements. The anticipated business impact of deploying this SaaS product is:

1. Onboard VBA personnel, in support of the PACT Act and it's Veterans
2. Reduce the administrative burden of hiring officials
3. Reduce hiring time and cost
4. Increase the efficiency in the hiring process.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

The HireVue GovCloud system limits sharing of information to those individuals who are given a role within the system to review the provided information. A role comparison matrix can be reviewed at https://app.hirevue.com/ui/hire-rap-chart/. It is at the discretion of the VA to determine if additional VA contractors or other agencies will be granted access to the system. HireVue personnel are provisioned access to the system following an access request process outlined in Access Control (AC)-2 in the HireVue GovCloud System Security Plan (SSP).

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

HireVue is a SaaS solution that is hosted on AWS GovCloud. HireVue's primary region is USWest, with the ability to failover to other AWS regions for business continuity services. HireVue has no additional information on the location of its data, as AWS does not share data center locations with clients.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Budget and Accounting Act of 1950 and General Accounting Office Title 8, Chapter 3. Social Security Numbers (SSN) are used to index and store pay affecting documents. SSNs are required from the customer for Internal Revenue Service (IRS) tax reporting and cannot be eliminated. SSNs are required for security clearance processing, which is authorized under Executive Orders 9397, 10450, 10865, 12333 and 12356; sections 3301 and 9101 of 5 U.S.C. and Homeland Security Presidential Directive 12."

"AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501, 7304.

SORN 1: Online Forms Submission-VA_SORN 211VA0478C 88 FR 911 - https://www.govinfo.gov/content/pkg/FR-2023-01-05/pdf/2022-28643.pdf

SORN 2: Veterans Affairs Profile-VA_192VA30 87 FR 36207 - https://www.govinfo.gov/content/pkg/FR-2022-06-15/pdf/2022-12864.pdf

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN will not require amendment or revision and approval.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*

No, this will not change the business process.

K. *Will the completion of this PIA could potentially result in technology changes?*

No, this will not result in any technology changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name ☐ Social Security Number ☐ Date of Birth

☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers
Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Biometrics

PII Mapping of Components (Servers/Database)

HireVue consists of **11** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **HireVue** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

HireVue GovCloud Interview Storage Components	Yes	Yes	First Name, Last Name, Biometrics	Storage of candidate interviews and provided files for review by hiring managers	Data encrypted in-transit and at-rest, access limited to need-to-know, components hardened against security baselines.
HireVue GovCloud Live Service	Yes	No	First Name, Last Name, Biometrics	Components that provide HIreVue OnDemand Video Interviews	Data encrypted in-transit and at-rest, access limited to need-to-know, components hardened against security baselines.
HireVue GovCloud OnDemand Service	Yes	No	First Name, Last Name, Biometrics	Components that provide HIreVue OnDemand Video Interviews	Data encrypted in-transit and at-rest, access limited to need-to-know, components hardened against security baselines.
HireVue GovCloud Web Application Database	Yes	Yes	First Name, Last Name	Store candidate responses/interview data for review by hiring managers	Data encrypted in-transit and at-rest, access limited to

					need-to-know, components hardened against security baselines.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

This information will be collected directly from the candidate while they complete their interviews. Additionally, VBA may opt to connect an Applicant Tracking System (ATS) to the HireVue web application, which will send PII via an encrypted ATS Connection.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

All data, whether entered from the candidate directly or from an ATS system, ultimately comes from the candidate. Data can be imported/exported to an ATS in order to better support tracking of candidates as they move through the job process.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The HireVue system is capable of storing scoring for candidates that are provided by members of the VBA Team assessing those candidates.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Data is collected directly from the candidates who complete interviews in the HireVue system. Candidates will provide name, email, and complete video interviews/assessments which will collect video and audio likeness. Additionally, data from an applicant tracking system (ATS) may be provided via an Application Programming Interface (API) connection in order to communicate when candidates are invited to and complete assessments.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is not collected on a paper form.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

HireVue has a number of the data provided by the candidate or the ATS has no additional checks for accuracy once ingested into the system.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, this system does not check for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

> AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Budget and Accounting Act of 1950 and General Accounting Office Title 8, Chapter 3. Social Security Numbers (SSN) are used to index and store pay affecting documents. SSNs are required from the customer for Internal Revenue Service (IRS) tax reporting and cannot be eliminated. SSNs are required for security clearance processing, which is authorized under Executive Orders 9397, 10450, 10865, 12333 and 12356; sections 3301 and 9101 of 5 U.S.C. and Homeland Security Presidential Directive 12."

"AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501, 7304.

SORN 1: Online Forms Submission-VA_SORN 211VA0478C 88 FR 911 -
https://www.govinfo.gov/content/pkg/FR-2023-01-05/pdf/2022-28643.pdf
SORN 2: Veterans Affairs Profile-VA_192VA30 87 FR 36207 -
https://www.govinfo.gov/content/pkg/FR-2022-06-15/pdf/2022-12864.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section)

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects, processes, and retains PII from members of the Public applying for opportunities at VA. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected, processed, and retained will be protected in accordance with FedRAMP Moderate controls and FIPS 140-2 encryption and data in-transit protection standards. All systems and VA users with access to the system will be approved, authorized, and authenticated before access is granted. Candidates will be provided a unique URL to complete their interview. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors. Cloud Service Provider annual privacy and security training compliance will be enforced by HireVue. RACI: Information System Security Officer (R); Privacy Officer (C); Information System Owner (C); VA Privacy Service (A).

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	*Internal Use*	*External Use*
Name	*File Identification purposes*	*Not used*
Personal Mailing Address	*Not Used*	*Not used*
Personal Email Address	*File identification purposes: contacting the candidate to take their HireVue interview*	*Not used*
Personal Phone Number	*Not Used*	*Not Used*
Biometrics	*Not Used*	*Not Used*

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

VA's instance of the HireVue application will analyze speech to transcribe. Hiring managers are able to review candidate responses and interviews and create comments and opt to rate responses, which are stored within the HireVue system. The HireVue system supports additional assessment and predictive scoring, but these features are not configured as part of the VA's tenant of the HireVue solution.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Any reports generated by HireVue based on the information provided by the candidate or entered by Hiring Managers will be stored within the HireVue application. Some reports can be downloaded directly to VA employee local devices, such as user lists for review by the VA Account Admin.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

HireVue ensures that all data at-rest (whether in S3 buckets or in HireVue's database) are encrypted via Key Management Service (KMS), which leverages FIPS 140-2 validated modules. Data in-transit across the internet is encrypted using Transport Layer Security (TLS) 1.2 using FIPS 140-2 validated modules, as long as the candidate/hiring manager uses a web browser that supports these ciphers. Non-FIPSed browsers will still ensure data is encrypted using TLS 1.2. Server to server communications within the HireVue environment are encrypted using FIPS 140-2 validated modules.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

Social Security Numbers will not be used.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

HireVue takes a number of steps to safeguard the data collected by HireVue GovCloud. These safeguards are based off of the FedRAMP Moderate Impact baseline of controls, and are reviewed as part of an annual assessment by HireVue's third-party assessment organization.

Account Creation: All access by HireVue personnel to HireVue GovCloud is reviewed and approved following a formal account lifecycle process. HireVue employees requesting access to the GovCloud system must first receive approval from their manager, HireVue's CISO or manager of Information Security, complete security and appropriate role-based training, and sign a set of Rules of Behavior. VA is able to control the creation and management of their user accounts through the account administrator role, ensuring that these accounts can be provisioned following the agency's process.

Information Flow: HireVue leverages various controls to limit the flow of client data in the HireVue system, including use of AWS security groups, VPCs, and subnets to limit what assets users can access when interacting with the system, and where client data flows.

Access Points and Remote Access: Users accessing the HireVue system are only able to do so through an AWS internet gateway. Access to infrastructure assets require authorized users to access HireVue's VPN, Bastion host, then access individual assets using SSH.

Awareness and Training: HireVue employees receive security awareness and training annually, and role-based training for individuals who can access federal data.

Configuration Management: HireVue GovCloud asset baselines are hardened to ensure unnecessary ports, protocols, services, and software are removed assets hosting client data. HireVue. HireVue reviews proposed changes to the assets and the environment and tests these changes following an SDLC process.

Encryption: All data in-transit and at-rest within HireVue GovCloud is encrypted using FIPS 140-2 validated ciphers. Information flows are enforced to ensure that data reside in appropriate areas of the system, including through limiting open ports and protocols on HireVue GovCloud assets,

Additional controls in place to protect the confidentiality, integrity, and availability of the HireVue GovCloud system can be reviewed in HireVue GovCloud's SSP.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: *Is the PIA and SORN, if applicable, clear about the uses of the information?*

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

For HireVue employees managing the HireVue GovCloud system, access is provisioned following the process outlined in AC-2 within the HireVue GovCloud SSP. Employee managers submit requests for access via a ticketing system. These tickets are reviewed and approved by the Chief Information Security Officer (CISO) or manager of information security and ensure the employee has completed the necessary security awareness training provided by HireVue, necessary role-based training offered by HireVue, and that the user has signed the necessary rules of behavior for access. HVAdmin or SSH accounts are only created once these conditions have been met.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

The VBA documents criteria, procedures, controls, and responsibilities regarding access.

For the platform, HireVue documents criteria, procedures, controls, and responsibilities regarding access to the HireVue GovCloud environment. Criteria and procedures are documented as part of HireVue's Information Security Management System (ISMS) documentations, as well as through the ticketing system's steps that are used to track user requests for access to the HireVue GovCloud platform. Controls are documented within the HireVue GovCloud SSP. Responsibilities are noted as part of HireVue's Acceptable Use and Rules of Behavior.

2.4c Does access require manager approval?

For HireVue employees, access requests must be submitted by the user's manager, and approved by either HireVue's CISO or manager of Information Security. Client accounts are the responsibility of the customer - VA Employees given access to VA's instance of the HireVue web application are able to follow the VA's account request process when having their accounts created.

2.4d Is access to the PII being monitored, tracked, or recorded?

HireVue GovCloud logs all access by users to the HireVue GovCloud environment, including the Username, IP, resources access, time of access, and access requests were successful or failed.

2.4e Who is responsible for assuring safeguards for the PII?

HireVue GovCloud's Information Security Team and Legal team are responsible for reviewing the security controls meant to safeguard information added to the HireVue GovCloud system.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

HireVue retains name, personal email address, and internet protocol (IP) address numbers.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information is retained in accordance with the General Records Schedule. Link: 2024 GRS.pdf. Per the General Records Schedule 2.1 Item 060, these are: Temporary. Destroy 1 year after date of submission.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes.

3.3b Please indicate each records retention schedule, series, and disposition authority?

Information is retained in accordance with the General Records Schedule. Link: 2024 GRS.pdf. General Records Schedule 2.1 Employee Acquisition Records: Item 060 and the Disposition Authority is DAA-GRS 2014-0002-0011.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

HireVue deletes candidate videos and overwrites PII fields in database entries with random data once retention periods have been reached.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.https://www.va.gov/vapubs/search_action.cfm?dType=1

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

The system is not used for research, testing or training.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: *Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?*

Principle of Data Quality and Integrity: *Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The system collects, processes, and retains PII from members of the Public applying for opportunities at VA. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: The HireVue system only collects, processes, and stores information on candidates related to the job search process, and not additional information such as sensitive PII (i.e. SSN), or PHI. Data is restricted to only those candidates invited to complete an interview. Data is collected, processed, and retained using FIPS 140-2. The HireVue Web Application can be configured to purge client data after a set retention period is passed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Human Capital Services	Talent Acquisition Services	● Last Name ● First Name ● Phone Number ● Personal Email ● Personal Address	Email. Secure File Transfer Protocol (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The system collects, processes, and retains PII on members of the public applying for career opportunities with the VA. If this information was breached or accidentally disclosed to inappropriate parties to the public as a result of inadequate internal sharing controls, it could result in personal harm to the individuals impacted and adverse negative impact to the VA.

Mitigation: The HireVue web application includes user permissions that restrict access to only those who have been given permission to review candidate interviews.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

HireVue (GovCloud Platform)	*Asset within the HireVue GovCloud system that ensures TLS connections to the HireVue system use FIPS 140-2 validated ciphers. As it is client communications across the internet, it must come into contact with candidate PII.*	● *First Name* ● *Last Name* ● *Email Address* ● *IP Address* ● *Biometrics*	*MOU/ISA*	*Data-in-transit is encrypted using TLS 1.2. No data-at-rest that is agency data. System hardened using DISA STIG Baselines, and ports/protocols/services limited to only needed functions. Access to system is monitored by HireVue's SecOps Team.*

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> If unauthorized access was gained from an external party (non HireVue employee) would cause a data breach; Allowing for the customers information to be accessed by an unauthorized party.

Mitigation:
VBA - This would be considered a privacy incident and would be entered in a data breach response system and an investigation would commence. The affected person would receive credit monitoring if needed.
HireVue – This would be considered a security incident and will be addressed following HireVue's documented incident response procedure.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?
These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

HireVue GovCloud includes a warning banner informing users that they are accessing a federal system and the user's actions are logged. Users are required to acknowledge these terms and conditions prior to beginning their interview.

Additionally, HireVue does allow for clients and agencies to configure additional terms and conditions and custom email templates to make sure candidates are aware of their privacy rights for their specific organization. These terms and conditions as well as emails can be configured to include agency privacy notices and requirements as needed. Reference screenshot below for the notice provided. HireVue Privacy Policy | HireVue.

SORN 1: Online Forms Submission-VA_SORN 211VA0478C 88 FR 911 - https://www.govinfo.gov/content/pkg/FR-2023-01-05/pdf/2022-28643.pdf

SORN 2: Veterans Affairs Profile-VA_192VA30 87 FR 36207 - https://www.govinfo.gov/content/pkg/FR-2022-06-15/pdf/2022-12864.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Users are informed of the collection prior to beginning their interview. HireVue Privacy Policy | HireVue.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Upon candidates' initial log on, they will receive this warning:

U.S. Government Notice
You are accessing a U.S. Government information system. By continuing, you consent to the following:

- ***The system may only be accessed and used for official Government business by authorized personnel.***
- ***Unauthorized access or use of this computer system is strictly prohibited and may be subject to criminal and civil penalties.***
- ***The system may monitor any activity, information, or communication on the system.***
- ***All activity, communication, and information on this system may be intercepted, recorded, read, copied, retrieved, audited, and disclosed by and to authorized personnel for official purposes, including criminal investigations.***
- ***Users have no right of privacy or any reasonable expectation of privacy in the use of this computer system and any communication or information stored within the system.***
- ***You have no reasonable expectation of privacy regarding any communication of data transiting or stored on this information system.***

Access or use of this system by any person, whether authorized or unauthorized, constitutes consent to all of these terms.

The applicant will then see the terms and conditions at this link: https://hirevue.com/terms/

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals can opt not to provide their personal information and not complete the digital HireVue interview process. If so, no alternate interview is offered as this is a refusal to participate and will be considered a declination to the interview. HireVue Privacy Policy | HireVue

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent *is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.*

HireVue provides its privacy policy for job candidate review at https://www.hirevue.com/legal/privacy. A link to these policies is included in emails sent to candidates.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Although sufficient notice has been provided to the individual, if unauthorized access was gained from an external party (non HireVue employee), it would cause a data breach and possible identify theft.
Mitigation:
VBA - This would be considered a privacy incident and would be entered in a data breach response system and an investigation would commence. The affected person would receive credit monitoring if needed.

HireVue – This would be considered a security incident and will be addressed following HireVue's documented incident response procedure (IRP).

HireVue's IRP for the HireVue GovCloud Platform:

- Provides the organization with a roadmap for implementing its incident response capability by defining members of the SIRT (distribution), roles and responsibilities in HireVue's incident response (under Roles) and provides both a high level view of the incident response process (under "Policies and Procedures"), as well as a deeper dive into each phase of HireVue's incident response capability (Identification, Containment, Eradication, Recovery, Follow-up).
- Includes processes for ensuring that affected Federal Agencies are notified of any incidents affecting their data
- Provides a high-level approach for how the incident response capability fits into the overall organization under the "Purpose" section, which describes the purpose of HireVue's IRP, and through the high-level procedure illustrated in the "Policies and Procedures" part of the document.

- Defines reportable incidents under the "Policies and Procedures" section of the IRP, which defines incidents as violations of HireVue's security and acceptable use policy (with additional examples provided).
- Defines the resources and management support needed to effectively maintain and mature an incident response capability under the "Roles" section of the IRP, which includes the responsibility of each individual or group in HireVue associated with the Incident Response process.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The Agency follows Federal FOIA/Privacy Act practices and procedures.

Below is information about requesting records from the Office of Accountability and Whistleblower Protection (OAWP). For more information, contact the Freedom of Information Act: https://department.va.gov/accountability/freedom-of-information-act-and-privacy-act-requests/how-to-make-a-freedom-of-information-act-foia-request/

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

No, the system is not exempt.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

This system is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

This information should be derived from USA Staffing as entered by the applicant. The responsible HR Liaison should be listed as the Point of Contact (POC). This will differ for each office.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

On the initial automated invite, applicants are advised of the process for needing support and/or correcting information by either reaching out to the hiring manager listed on the automated invite and/or contacting HireVue support at support@hirevue.com.

More information on HireVue's process is listed below:

As the data processor, HireVue will route all requests around redress and compliant management to the data controller (the federal agency). It is the responsibility of the data controller to ensure individuals are made aware of their ability to correct their information in accordance with VA's privacy program.

Details on this process and how candidates can make requests around their data are shared in HireVue's publicly available privacy policy, which is located at https://www.hirevue.com/legal/privacy. Specifically, the candidates right around the candidates rights to correct their information is provided under section "Your Data Protection Rights", available at https://www.hirevue.com/legal/privacy#your-data-protection.

Additionally, the HireVue system includes the ability for candidates to include additional terms/conditions/additional verbiage specific to their organization prior to the candidate beginning the interview process, allowing for VBA to place additional privacy notices specific to their agency.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Per above, formal redress is provided.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

<u>Principle of Individual Participation:</u> Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

<u>Privacy Risk:</u> There is a risk that the applicant will provide incorrect applicant information while their application is in processing and the applicant would not be notified of pending interviews for a potential open position.

<u>Mitigation:</u> The HireVue system does provide data validation that helps enforce correct data (i.e. telephone number, email address formatting).

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

All access by HireVue personnel to HireVue GovCloud is reviewed and approved following a formal account lifecycle process. HireVue employees requesting access to the

GovCloud system must first receive approval from their manager, HireVue's CISO or manager of Information Security, complete security and appropriate role-based training, and sign a set of Rules of Behavior. VA is able to control the creation and management of their user accounts through the account administrator role, ensuring that these accounts can be provisioned following the agency's process.

Candidates: Candidates receive an email inviting them to complete an interview via a URL link.

VA Personnel: VA can follow the process they desire to provision access to VA employees who need to access this solution. There is no limit on user licenses, and user accounts are created by the customer.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users from other agencies will not have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Account Admin: Full access to everything within the account.
Key Functionality:

- Can access and edit all positions and interviews.
- Run reports across all teams.
- Manage account users as well as account settings.

Account Admin Limited: Access to everything within the account except for the ability to administer users.
Key Functionality:

- Can access and edit all positions and interviews.
- Run reports across all teams.

User Manager: Administer users and manage accounts.
Key Functionality:

- Manage account users as well as account settings.

Tip: Use this role for team members who are not everyday users of HireVue but may need to administer users.

Team Admin: See and edit all candidates and positions within that team.
Key Functionality:

- Can access and edit all positions on their team.
- Can create new questions and save Question Templates.
- Can add or remove team members from their teams.
- Run reports across their teams.
- Can edit Team Settings.

Team Collaborator: Full permissions to edit and manage all positions in their team just as if they had created the positions themselves.

Key Functionality:

- Can access and edit all positions on their team.
- Cannot run reports.
- Cannot edit team settings.
- Cannot add or remove team members.
- Can view HireVue Assessments scores.

Tip: Use this role for users who need to work cross functionally on positions but don't need full access to everything on the team.

Please note: If this role is not listed on your account, reach out to your Customer Success Manager (CSM).

Team Collaborator – Limited: Load existing questions in a position from either a question template, previous position or question bank.

Key Functionality:

- Can access and edit all positions on their team and assign assessment models.
- Can load existing questions from question banks, templates, or previous positions.
- Can view HireVue Assessments scores.
- Cannot create new questions or templates.

Tip: Use this role for users who need to work cross functionally on positions but don't need full access to everything on the team or access to create questions or templates.

Team Reporting Manager: Permissions to edit and manage all positions within their team and manage reporting.

Key Functionality:

- Can access and edit all positions on their team.
- Can view HireVue assessments and scores.
- Can view, download, and share reports.
- Cannot edit team settings.
- Cannot add or remove team members.

Team Member: See and edit only their own position.

Key Functionality:

- Can create and manage their own positions.
- Can create new questions and save Question Templates
- Cannot run reports.
- Cannot edit team settings.
- Cannot add or remove team members.

Team Member – Limited: Ability to load existing questions into their own positions from either a question template, previous position, or a questions bank.

Key Functionality:

- Can load existing questions into own position.
- Can load questions from templates, question banks, or previous positions.
- Cannot create new questions or templates.

Tip: Use this role for users who need a Team Member type role but don't need access to create questions or templates.

Hiring Manager: Read only view of positions that are explicitly shared with them.
Key Functionality:

- Evaluate assigned candidates.
- Some ability to manage evaluators and candidates for positions.
- View notes, ratings, and recommendations from other evaluators
- View comparison chart
- See interview details such as questions and interview set up.

Tip: Use this role for users who only need to review candidates but not create or manage positions.

Sourcer: Read only view of positions that are explicitly shared with them.
Key Functionality:

- Can add new candidates but can only see the candidate they've added themselves.
- Can watch interviews of the candidates they've added.
- Can evaluate candidates if they are assigned to the position as an evaluator.

Tip: Use this role for users who work with outside agencies for sourcing candidates.

Evaluator: Participate and evaluate interviews that have been assigned to them.
Key Functionality:

- Evaluate assigned candidates.
- Cannot view evaluation data from other evaluators.

Please note: This is a default role that a user is assigned when they are added as an evaluator to review a candidate interview within HireVue.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Non-VA employees, other than HireVue, will not have system access to HireVue.

HireVue houses the candidate's first name, last name and email address.

Each contract is reviewed once per year.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

VA Privacy & Security training, as well as HireVue systems training dependent upon the user's role.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 1/29/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 5/24/2024
5. *The Authorization Termination Date:* 5/8/2025
6. *The Risk Review Completion Date:* 7/25/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not applicable.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

This system is a Software as a Service (SaaS) that uses cloud technology, specifically AWS GovCloud. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR1831429369.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of* *the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, the contract establishes who has ownership rights over data, including PII. The contract between the VA and the SaaS vendor (HireVue)—there is no contractual agreement between the VA and the CSP—states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is # NNG15SD43B (order number is 36C10D23F0049).

IT security information is in section C.2 of the contract with references about rights in data noted in section 3.a – VA INFORMATION CUSTODIAL LANGUAGE. This section includes the following:

Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

*copy of contract provided

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

The HireVue GovCloud systems collects logging data of candidate and user IP addresses, usernames, when the system is accessed, what actions are taken, and the result of all actions taken within the web application. HireVue collects this data to monitor the security of the application and alert on anomalous activity. HireVue has ownership over this data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, this is in the contract for the implementation of HireVue in the FedRAMP authorized environment.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

HireVue does not use robotics process automation to modify or read candidate PII.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response

ID	Privacy Controls
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2024.09.12 15:00:28 -05'00'

Privacy Officer, Marvis Harvey

ALBERTINO ESTACIO Digitally signed by ALBERTINO ESTACIO
Date: 2024.09.18 14:42:57 -07'00'

Information Systems Security Officer, Albert Estacio

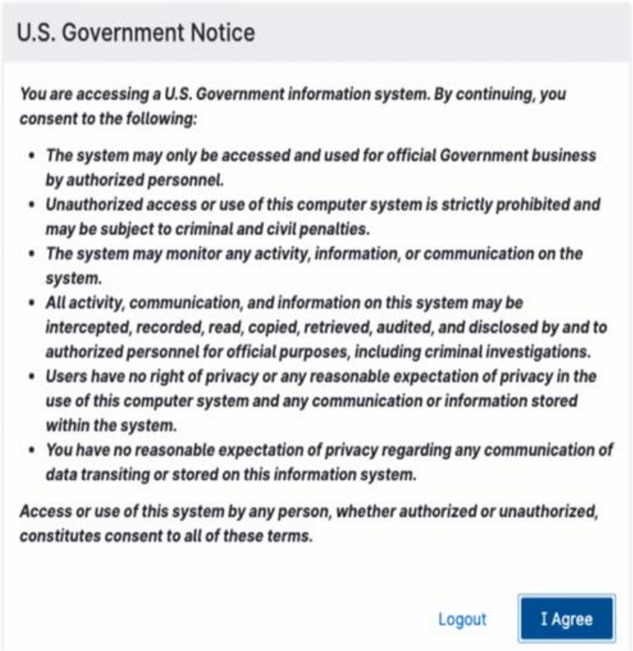
CHINO WALTERS Digitally signed by CHINO WALTERS
Date: 2024.09.20 10:25:13 -04'00'

Information Systems Owner, Chino Walters

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HireVue Privacy Policy | HireVue



U.S. Government Notice

You are accessing a U.S. Government information system. By continuing, you consent to the following:

- *The system may only be accessed and used for official Government business by authorized personnel.*
- *Unauthorized access or use of this computer system is strictly prohibited and may be subject to criminal and civil penalties.*
- *The system may monitor any activity, information, or communication on the system.*
- *All activity, communication, and information on this system may be intercepted, recorded, read, copied, retrieved, audited, and disclosed by and to authorized personnel for official purposes, including criminal investigations.*
- *Users have no right of privacy or any reasonable expectation of privacy in the use of this computer system and any communication or information stored within the system.*
- *You have no reasonable expectation of privacy regarding any communication of data transiting or stored on this information system.*

Access or use of this system by any person, whether authorized or unauthorized, constitutes consent to all of these terms.

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices