



Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "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." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 551

System Name: GSA Implementation of Recruitment Assessments and Video Interviewing

CPO Approval Date: 9/21/2026

PIA Expiration Date: 9/20/2029

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:

GSA Implementation of Recruitment Assessments and Video Interviewing

B: System, application, or project includes information about:

C: For the categories listed above, how many records are there for each?

D: System, application, or project includes these data elements:

Overview:

GSA Client:

- Federal Acquisition Services (F) - Technology Transformation Services (TTS)

System, application, or project includes information about:

- The public

System, application, or project includes these data elements:

- Contact information (full name, telephone number, email address)

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

The Government seeks to acquire a commercially available, cloud-based technical assessment platform to support skills-based evaluation and assessment activities in compliance with the President's January 20, 2025 Executive Order 14170 "Reforming the Federal Hiring Process and Restoring Merit to Government Service" and the "Merit Hiring Plan" implementation. The solution will be used to evaluate technical competencies efficiently and consistently using industry-standard tools and methodologies. The requirement is for a subscription-based Software-as-a-Service (SaaS) offering and does not include custom software development. PII is collected from individuals external to GSA who have applied for open positions on USAjobs and were deemed eligible after a resume review. Individuals who are not employed by GSA but are seeking employment are designated as External Candidates and are provided a unique link to create their applicant account using their name and email address. The email address serves as a unique identifier that connects the applicant to their interview assessment information

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?

Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?

Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

OPM/GOVT-5 Recruiting, Examining and Placement Records

OPM/GOVT-6 Personnel Research and Test Validation Records

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.

The active life expectancy of the data in HireVue is for the duration of the active identity account, which could be for the duration of the individual's employment/assignment.

The GSA Records Retention Officer and the Department of Homeland Security developed the "GSA Personal Identity Verification IDMS Record Retention and Disposition Schedule" document for data retention schedules.

As indicated, the retention requirements are a minimum of five years from the date when the identity account moves from an active to inactive status (month of separation). Disposition of records will be according to NARA disposition authority N1-269-06-1 (pending).

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?

HireVue collects email addresses to serve as the unique identifier for each user and form of communication between the onboarding team and external candidates. There are no non-PII equivalent would not be sufficient since some form of identify proofing is required to ensure the applicant information matches what is on file within the HR system that store more sensitive PII like SSN and home addresses

3.2: Will the system, application, or project create or aggregate new data about the individual?

No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

The HireVue platform employs a defense-in-depth strategy, integrating technical, managerial, and operational security controls to protect consolidated data and prevent unauthorized access.

Access and Authentication Controls

- **Authentication:** Internal GSA users authenticate through GSA Auth (Okta) using multi-factor authentication (MFA) via PIV or approved second-factor methods (e.g., Okta Verify, SNA tokens). External candidates access the system via individualized, unique tracking identifiers and invitation links, which do not provide system-level or network-level access.
- **Role-Based Access Control (RBAC):** Access is governed by least-privilege principles. System roles and associated privileges are strictly defined, and access is provisioned through controlled workflows (SailPoint).
- **Session Management:** The system enforces session locks after 15 minutes of inactivity and requires re-authentication after 30 minutes of inactivity or 12 hours of continuous usage.

Network and Technical Security

- **Boundary Protection:** The production environment utilizes a Web Application Firewall (WAF) (Signal Sciences) to inspect HTTPS traffic, block malicious web application traffic, and prevent OWASP attacks.
- **Logical Segregation:** The HireVue GovCloud environment is logically segregated within AWS GovCloud VPCs to prevent unauthorized transfer of information via shared resources.
- **Internal Hardening:** Host-based firewalls (AWS security groups) are configured with a deny-all/permit-by-exception methodology, allowing only authorized traffic between system components.
- **System-Level Protections:** The production environment uses multi-state processor technologies to ensure process isolation, memory protection, and comprehensive input validation to protect resource availability.

Managerial and Lifecycle Oversight

- **Account Lifecycle Management:** Access is managed through SailPoint-driven processes. Privileged accounts undergo quarterly access reviews, while standard accounts are reviewed annually to verify continued need.
 - **Offboarding:** Accounts are promptly disabled or removed following HR-initiated offboarding, with the System Owner and ISSO reconciling active accounts against HR records monthly.
-

- **Data Identification:** The system relies on internal unique record IDs rather than external identifiers (e.g., social security numbers or contract numbers), ensuring that PII is not retrieved via personal identifiers as a standard operational practice.

Monitoring and Incident Response

- **Continuous Monitoring:** All system activity generates audit logs that are forwarded in real-time to a Security Operations Center (SOC) dashboard and analyzed via Splunk.
- **Incident Response:** Suspected or confirmed incidents are handled in accordance with GSA and HireVue incident response procedures, which include mandatory reporting to CISA/US-CERT and contractual obligations for HireVue to notify GSA of incidents "without undue delay".

3.4 Will the system monitor the public, GSA employees, or contractors?

Public

3.4 Explain: Please elaborate as needed.

HireVue's monitoring activity is limited to individuals participating in the hiring/assessment process and to GSA users who access the system; it is not used for general surveillance of the public, the existing workforce or contractors performing unrelated duties.

3.5 What kinds of report(s) can be produced on individuals?

N/A

3.6 Will the data included in any report(s) be de-identified?

No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?

HireVue generates evaluation reports that grade each applicant based on how the evaluators score their assessment. These scores are used to determine which applicants will move forward in the hiring process.

Whether report data is de-identified depends on the report type and its purpose. Individual-level hiring reports are not de-identified, as identification is necessary to support the hiring decision they inform.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?

None

4.2How: If so, how will GSA share the information?

No

4.3: Is the information collected:

Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?

No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?

No

4.4NoAgreement: Why is there not a formal agreement in place?
formal agreement is not required

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Accuracy and completeness of information in HireVue are addressed through a combination of applicant self-certification, system-level controls, and HR review processes, as follows based on Hirevue Assessments Overview Whitepaper and Hirevue AI Explainability Statement:

Applicant-Provided Information

The majority of information in the system (resume/application data, responses to interview questions, self-reported qualifications) is entered directly by the applicant. Accuracy is primarily the responsibility of the individual providing it:

- Applicants certify the accuracy of their application materials at submission, consistent with standard federal employment application certification language (e.g., false statements may be grounds for non-selection or removal)
- Applicants are able to review responses/materials before final submission within the HireVue platform.

System-Generated Information

Video/audio recordings and any automated assessment scores are generated directly by the platform at the time of the applicant's interaction, which limits transcription or data-entry error since there is no manual re-entry step between the applicant's response and the stored record.

Capture and Ingestion Architecture

Media Stream Capture: Client browsers or mobile applications record audio/video streams locally via standard web APIs, uploading packets directly to cloud storage endpoints upon completion of each question block.

Session Telemetry: The platform logs interaction metadata, timing parameters, and browser focus-loss events (such as tab switching) directly into the assessment database.

No Human-in-the-Loop: Recordings are placed straight into secure cloud object storage without any manual cutting, routing, or intermediate human processing.

Automated Processing and Storage Pipeline

Speech-to-Text Engine: Audio files pass through an automated transcription pipeline that converts spoken candidate responses into structured text strings.

Natural Language Processing (NLP): Large Language Models (LLMs) and deterministic text models analyze the text transcript mathematically to evaluate job-related competencies.

Static Scoring Output: Pre-trained, locked algorithms evaluate the text against criteria established by industrial-organizational (I/O) psychologists, outputting stack-rank scores and tier bands directly to the employer dashboard alongside the raw media files.

HR Review and Quality Control

GSA HR staff and hiring officials review applicant-submitted information as part of the qualification and eligibility determination process, providing a secondary check on completeness (e.g., flagging incomplete applications) though not on the underlying truthfulness of applicant-provided content.

Dissemination

Information disseminated to hiring officials or interview panels is drawn directly from the candidate materials available within the HireVue system. Access is not uniform across all users; hiring officials, evaluators, and team administrators must possess an active, approved identity profile within GSA SailPoint mapping to the explicit role configurations defined in [Table 9-3](#) of the SSPP. Because access is strictly gated by these role-based configurations and no additional manual processing is performed, the information provided to officials reflects the underlying candidate submissions without introducing additional accuracy or compliance risk.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

Authorized access to the system for internal GSA employees is determined through multi-factor authentication and role enforcement synchronized via the GSA Auth SSO (Okta) platform. GSA-internal employees must submit access requests directly through the front-end [GSA SailPoint Self-service Portal](#) utilizing either the "Request for Yourself" or "Request for Others" pathways. The platform automatically routes an approval notification email to the applicant's designated supervisor; upon supervisor approval, a second-level automated notification is sent to the HireVue Administrator group for final verification and manual console provisioning.

6.1b: What is the authorization process to gain access?

Account administrators from HR, Onboarding, various program offices, the System Owner, and the ISSO will have role-based access to candidate work products and evaluation scores. The System Owner receives monthly HR offboarding spreadsheets and reviews them against active internal accounts. Any user appearing on the agency separation list is promptly deactivated and removed from the system in accordance with GSA CIO-IT Security-01-07.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
9/21/2026

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?

Authorized access for GSA internal users to the system is determined through authentication and authorization enforced by the GSA Auth SSO (Okta) platform. Users external to GSA do not hold logical accounts and are provided a secure, tokenized link via email to access their specific technical evaluation session for a finite period of time.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?

Yes

6.4What: What are they?

GSA and HireVue maintain layered mechanisms to detect, report and respond to security incidents and breaches involving PII, consistent with GSA IT Policy and applicable federal breach response requirements.

Suspected or confirmed security incidents are identified through automated alerting, vendor notification, or user/staff reporting, and are handled in accordance with GSA's incident response procedures.

Incident Response Process

- GSA personnel and contractors are required to report suspected incidents involving PII within required timeframes (per US-CERT/CISA reporting requirements, generally within 1 hour of discovery for confirmed incidents)
- HireVue, as the SaaS provider, is contractually obligated to notify GSA of any suspected or confirmed incident affecting GSA data within a specified timeframe.

Reporting to External Authorities

- Confirmed incidents involving PII are reported to the U.S. Computer Emergency Readiness Team (CISA/US-CERT) within required timeframes.
- Incidents are also reported to the GSA Office of Inspector General (OIG) and/or Congress, as applicable, per current OMB and GSA policy

Notification to Affected Individuals

If a breach is determined to pose a risk of harm to affected individuals, GSA's Breach Response Team determines appropriate notification method, content, and timing in accordance with OMB M-17-12 and GSA Information Breach Notification policy.

Contractual/HireVue (SaaS-Specific Controls)

As a cloud/SaaS system, HireVue's incident response procedures and breach notification obligations to GSA are governed by the underlying contract and Security incident reporting and procedures are detailed in Hirevue's Incident Response Plan and Data Processing Addendum:

Notification: Upon becoming aware of a Security Incident, HireVue must notify the Buyer (GSA) "without undue delay".

Response and Remediation:

HireVue will provide reasonable information and cooperation to assist the Buyer in fulfilling any data breach reporting obligations it may have under applicable law.

HireVue is responsible for taking reasonably necessary measures or actions to minimize the impact of the incident.

HireVue will keep GSA informed of all material developments regarding the incident.

Training: HireVue implements a security awareness program for its personnel that includes training regarding security practices and security incident reporting.

Audit Rights: Following a Security Incident, the Buyer (or its appointed third-party auditors) is permitted to carry out an audit of HireVue's processing of Personal Data.

The response process is managed by the Security Incident Response Team (SIRT) and follows these primary phases:

Detection and Investigation: Incidents are identified through automated alerting, vendor notification, or user/staff reporting. Incidents are categorized by severity (Critical, High, Moderate, or Low) based on the impact to system availability and customer data.¹

Containment: The infrastructure department secures the network perimeter and retrieves volatile data to ensure evidence is preserved.

Eradication and Recovery: The SIRT removes the root cause of the exposure, verifies the fix through vulnerability assessments, and restores systems to their "last known good" state.¹

Follow-up: Responders review the incident to identify "lessons learned" and potential process improvements.

Notification: HireVue is contractually obligated to notify customers of confirmed data breaches "without undue delay".

In the USOnly/FedRAMP environment, HireVue reports incidents to the sponsoring agency, Agency Authorizing Official (AO), and Agency Incident Response Team within one hour of discovery.

Incident/Breach Response Exercises

To ensure the effectiveness of the incident response process, HireVue incorporates the following simulation and testing activities:

Annual Tabletop Exercises: HireVue conducts incident response tabletop exercises annually. These exercises are designed specifically to test the plan and identify areas for improvement.

Tracking and Documentation: Participation is tracked, including the name of the employee and the date the exercise was completed.

Refinement: Results, materials used, and lessons learned from these exercises are used to refine the Incident Response Plan. Upon completion of annual incident response testing, details—including the participants and the materials used—are recorded within the incident response ticket system.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

Individuals do not have a general right to opt out of providing information while remaining under consideration for a GSA position. Providing information to HireVue is voluntary only in the broad sense that no one is required to apply for a GSA position; once an individual applies for a vacancy that uses

HireVue as part of the assessment or interview process, completing the requested video interview, assessment, or associated data collection is a required condition of continued consideration

7.1Opt: Can they opt-in or opt-out?

No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Individuals do not have a general right to opt out of providing information while remaining under consideration for a GSA position. Providing information to HireVue is voluntary only in the broad sense that no one is required to apply for a GSA position; once an individual applies for a vacancy that uses HireVue as part of the assessment or interview process, completing the requested video interview, assessment, or associated data collection is a required condition of continued consideration. Declining to provide the information results in the applicant not being able to proceed further in that competitive process — it does not trigger a data-handling opt-out while otherwise remaining in consideration.

7.2: What are the procedures that allow individuals to access their information?

Candidates will be able to view their profiles and assessment after creating an account via their designated invitation link for an allotted period of time. After that the individual will not have access to their information.

7.3: Can individuals amend information about themselves?

Yes

7.3How: How do individuals amend information about themselves?

Yes, outlined in Privacy Policy:

<https://www.hirevue.com/company/privacy>

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All GSA employees and contractors are required to complete an annual IT Security & Privacy Refresher Training in the Online Training University.

This course comprises 4 modules: IT Security Awareness Training, Sharing Securely in a Collaborative Environment, Safeguarding GSA Sensitive Information, and IT Rules of Behavior.

The information in these modules are updated yearly.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?

Authentication and authorization controls are in place to manage appropriate access to systems and data. The System Owner will limit access Account Administrators access to external candidate information so that each admin can only view information on candidates within their some team (e.g. admins from [Login.gov](https://login.gov) can only view information from candidates applying to positions within Login.gov)