United States Department of Justice (DOJ)
Office of Attorney Recruitment and Management (OARM)

# Privacy Impact Assessment
# for the
# Avue Digital Services

Issued by:
Office of Attorney Recruitment and Management Deputy Director
Michael Stamp

Approved by: Brian Young
Acting Deputy Director, Office of Privacy and Civil Liberties

Date approved: January 31, 2025

*(May 2022 DOJ PIA Template)*

*[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]*

## Section 1: Executive Summary

***Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)***

Avue Digital Services (Avue) is a personnel management system provided by Avue Technologies Corporation that allows the Department of Justice (DOJ) Office of Attorney Recruitment and Management (OARM) to manage centralized hiring programs for entry-level attorneys (Attorney General's Honors Program or HP) and compensated legal interns (Summer Law Intern Program or SLIP) and allows job applicants to apply for employment during an annual recruitment cycle. In addition, Avue is a managerial portal where OARM can review applicant eligibility, track hiring by multiple components throughout the hiring cycle, conduct outreach to fill ad hoc vacancies during the 10 months the application remains active, communicate with applicants, post real-time status updates, and generate aggregate application workflow data.

Applicants may create an account and submit applications during the annual open season (typically July 31 through the Tuesday after Labor Day). DOJ employees in participating components can log into the Avue webpage with credentials that are created by Avue after OARM staff submit a user management request.

OARM has prepared a Privacy Impact Assessment for Avue because this system collects, maintains, and disseminates information in identifiable form about job applicants and DOJ employees, to include privacy-sensitive information that an applicant would provide (*e.g.,* the applicant's name, address, phone number, e-mail address, education, legal practice areas of interest, qualifications, work experience, veterans preference eligibility, other information that is considered employment-related, and, at the applicant's discretion, sex, race, national origin (RSNO), ethnicity, disability information). Social security numbers are not collected by OARM or Avue as part of the application process.

## Section 2: Purpose and Use of the Information Technology

***2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.***

OARM manages the Attorney General's Honors Program and Summer Law Intern Program. As part of its management functions, OARM contracts with Avue for its services. Avue provides

OARM with an online application and applicant management system tailored specifically for the HP and SLIP in a Software as a Service (SaaS) solution. Specifically, job applicants use the system to apply online and OARM personnel and authorized DOJ hiring organizations use the system as a managerial portal to oversee the hiring process. Position and applicant information will be shared, as is necessary and appropriate, with Component Human Resources (HR), managers, selecting officials, and hiring committees.

Personally Identifiable Information (PII) is available only to users who have a need-to-know, and who have appropriate permissions, when viewing information in the system and when generating reports (e.g., application summaries, qualifications "dashboards," etc.). Applicant information is shared with designated DOJ human resources staff, managers, selecting officials, and other agency employees or contractors involved in the selection process. Only users with appropriate role-based access and permissions are able to generate reports containing PII. Additionally, OARM approves any requests for new accounts.

Avue collects applicant data directly from applicants, who may include members of the general public and current federal employees (*e.g.*, current DOJ HP attorneys in time-limited positions who remain eligible). Applicant information may include names, addresses, telephone numbers, e-mail addresses, race, sex, national origin, ethnicity, disability information and other sensitive information related to employment, education, and other information relevant to the jobs for which the individual applies.

The routine use of the information is to evaluate individuals for specific employment opportunities as well as to facilitate the selection process. Any RSNO, ethnicity or disability information that is voluntarily provided by applicants in aggregate form is not linked to the individual's application and is only used by OARM for programmatic evaluation and in the form of summaries that are provided to participating components for evaluation.

### *2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

| Authority | Citation/Reference |
|---|---|
| Statute | 5 U.S.C. Part II, Ch 11, Section 1104<br>34 U.S.C. § 10226 |
| Executive Order | |
| Federal regulation | 28 C.F.R. § 0.138; 28 C.F.R. § 0.15 |
| Agreement, memorandum of understanding, or other documented arrangement | |
| Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A, B, C and D | Full names of applicants (which may include Department of Justice employees and other Federal employees) are collected. |
| **Date of birth or age** | | | |
| **Place of birth** | | | |
| **Sex** | X | A, B, C and D | Sex is collected (voluntary) |
| **Race, ethnicity, or citizenship** | X | A, B, C and D | Race and origin information of applicants is collected (voluntary) |
| **Religion** | | | |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | | | |
| **Tax Identification Number (TIN)** | | | |
| **Driver's license** | | | |
| **Alien registration number** | | | |
| **Passport number** | | | |
| **Mother's maiden name** | | | |
| **Vehicle identifiers** | | | |
| **Personal mailing address** | X | A, B, C and D | Personal mailing address is collected. |
| **Personal e-mail address** | X | A, B, C and D | Personal email address is collected. |
| **Personal phone number** | X | A, B, C and D | Personal phone number of applicants is collected. |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account information** | | | |
| **Applicant information** | X | A, B, C, and D | This information is collected during the application process. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Education records** | X | A, B, C, and D | Information about education history (college, law school, other graduate school is collected and applicants upload a law school transcript during the application process. |
| **Military status or other information** | X | A, B, C, and D | Applicants provide military status and may upload military service records, such as the DD 214 and VA disability documents (e.g., Summary of Benefits letter) during the application process. |
| **Employment status, history, or similar information** | X | A, B, C, and D | Applicants provide employment status during the application process |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | | | |
| **Certificates** | | | |
| **Legal documents** | | | |
| **Device identifiers, e.g., mobile devices** | | | |
| **Web uniform resource locator(s)** | | | |
| **Foreign activities** | | | |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | | | |
| **Juvenile criminal records information** | | | |
| **Civil law enforcement information, e.g., allegations of civil law violations** | | | |
| **Whistleblower, e.g., tip, complaint, or referral** | | | |
| **Grand jury information** | | | |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | | | |
| **Procurement/contracting records** | | | |
| **Proprietary or business information** | | | |
| **Location information, including continuous or intermittent location tracking capabilities** | | | |
| ***Biometric data:*** | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - **Photographs or photographic identifiers** | | | |
| - **Video containing biometric data** | | | |
| - **Fingerprints** | | | |
| - **Palm prints** | | | |
| - **Iris image** | | | |
| - **Dental profile** | | | |
| - **Voice recording/signatures** | | | |
| - **Scars, marks, tattoos** | | | |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | | | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **User ID** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **User passwords/codes** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **IP address** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **Date/time of access** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **Queries run** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| - **Contents of files** | X | A, B, C, and D | Web activity is collected and monitored by Avue Technologies IT Operations Team. |
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C, and D | Web cookies used for session management are collected. |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

| **Directly from the individual to whom the information pertains:** | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | | Online | X |

| | | | | | |
|---|---|---|---|---|---|
| Phone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | | Other DOJ Components | | Other federal entities | |
| State, local, tribal | | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | | | |
| Other (specify): | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | X | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): | | | | | |

## Section 4: Information Sharing

***4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.***

| **Recipient** | **How information will be shared** | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | | | X | Application materials collected in Avue are made available to OARM staff. PII is only available to staff with a need-to-know and is secured by access controls (accounts are provisioned based on roles and permissions, and the principle of Least Privilege is used; end users only see data and perform tasks based on the access to the system required for that end user account). |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| DOJ Components | | | X | Application materials collected in Avue are made available to OARM-authorized human resources staff, managers, selecting officials, assessment panels, and other agency employees or contractors involved in the selection process. PII is only available to staff with a need-to-know and is secured by access controls (accounts are provisioned based on roles and permissions, and the principle of Least Privilege is used; end users only see data and perform tasks based on the access to the system required for that end user account). |
| Federal entities | | | | |
| State, local, tribal gov't entities | | | | |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | | | | |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | | | | |
| Other (specify): | X | | | Applicants self-provision (i.e., create their own account) when they register to begin the application process. Applicants can contact the Avue Help Desk for support. |

***4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

N/A

## Section 5: Notice, Consent, Access, and Amendment

***5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.***

The system will provide both a generalized notice to the public as well as a statement that complies with the Privacy Act. Avue displays its Privacy Policy on its website. Among other things, it lists the authorities with which it maintains compliance as a generalized notice to the public. Additionally, information will be provided through a Privacy Act Statement that complies with 5 USC § 552a(e)(3), and this Privacy Impact Assessment will be published, maintained, and updated as needed on the Department's Office of Privacy and Civil Liberties website.

The following SORNs have been published in the Federal Register and provide broad public notice:

OPM/GOVT-1 - General Personnel Records, 71 FR 35356 (June 19, 2006) (as modified by 77 FR 73694 (Dec. 11, 2012)).

OPM/GOVT-5 - Recruiting, Examining, and Placement Records, 79 FR 16834 (Mar. 26, 2014) (as modified by 80 FR 74815 (Nov. 30, 2015); and 86 FR 68291 (Dec. 1, 2021).

***5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

Providing the information requested by DOJ/OARM on the federal employment application is voluntary; however, failure to provide it may result in a determination of ineligibility or disqualification from consideration. Users may contact the Avue Help Desk if they do not consent to using the application to obtain instructions for reasonable accommodations on a case-by-case basis.

***5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.***

Prior to the application deadline, Avue users can validate or modify personal information through the standard user interface. As provided in the OPM System of Records Notice (SORN), individuals seeking to contest or amend records post-deadline must directly contact the applicable component's FOIA Officer. Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the

"Record Access Procedures" paragraph in the SORN. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

The applicant or employee end users can also gain access to their information from Avue and, prior to the deadline, correct any errors with the assistance of the Avue Help Desk. End users must verify that their information is accurate and that individual Rules of Behavior are followed. The Avue Help Desk is staffed by Avue employees with appropriate permissions and role-based access. The Avue Help Desk has access to information that an applicant provides such as name and contact information as indicated in Section 3.1. The integrity of personnel data is checked by reviewing it with OARM. The applicant and employee end users may correct inaccurate PII following a review of information. Additionally, PARs can be processed to correct or amend inaccurate PII.

## Section 6: Maintenance of Privacy and Security Controls

***6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).***

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):**<br>Avue Digital Services (ADS) – ATO Date: 3/21/22; Expires: 3/21/2025<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**<br>Avue is a SaaS product and as such POA&Ms related to the cloud platforms FedRAMP packages are stored in the U.S. Department of Agriculture (USDA) Connect.gov due to sensitivity. |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |

| | |
|---|---|
| | **This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:**<br>N/A |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**<br>As part of its FedRAMP authorization, Avue has implemented a continuous monitoring program, where security controls and risks are assessed, and all system components scanned for vulnerabilities and validated monthly to support risk-based security decisions to adequately safeguard OARM data. Avue processes are assessed and validated annually by a FedRAMP authorized third-party assessment organization (3PAO). Avue acknowledges that any suspected/confirmed incident or breach to the system will be reported to the Contracting Officer Representative and Justice Security Operations Center (JSOC). |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:**<br>Avue provides logs to OARM on request for audit and review. These logs are updated and available monthly via Connect.gov as part of the Avue Continuous Monitoring Program. |
| | **Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.<br>N/A |
| | **Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:**<br>OARM provides training specific to Avue's HP/SLIP program management to component users (DOJ employees) annually. |

***6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

Avue has a Federal Information Processing Standard Publication 199 (FIPS-199) security categorization of Low due to the staff acquisition information that it contains. A full security control assessment has been completed for Avue, to include physical access, identification and

authentication, vulnerability management, auditing, etc. Avue makes use of separation of duties for Privileged and Non-Privileged user accounts and leverages additional role-based access control technologies and administrator session recording. All system and application log data is being sent to an internal General Support System's centralized audit log management system for triage and review. Avue users connect to the Amazon Web Services (AWS) hosted environment over a secure VPN tunnel between the user's workstation and an OpenVPN server. All traffic through this tunnel uses Secure Socket Layers (SSL)/Transport Layer Security (TLS) to protect the confidentiality and integrity of transmitted information. SSL/TLS provides the confidentiality and integrity of transmitted traffic and ensures that passwords are encrypted. End Users connect to Avue over an HTTPS connection which is FIPS-140-2 certified. All weak ciphers, or algorithms, are removed and strong ciphers are prioritized to ensure compliance with Federal and Department guidelines.

***6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)***

Records in this system are retained and disposed of in accordance with the National Archives and Records Administration, General Records Schedule Section 2.1: Employee Acquisition Records. Records in this system are retained for varying lengths of time, ranging from a few months to a maximum five years. Some records, such as individual applications, become part of the person's permanent official records when hired.

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

_____ No. __X__ Yes.

***7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

OPM/GOVT-1 - General Personnel Records, 71 FR 35356 (June 19, 2006) (as modified by 77 FR 73694 (Dec. 11, 2012)).

OPM/GOVT-5 - Recruiting, Examining, and Placement Records, 79 FR 16834 (Mar. 26, 2014) (as modified by 80 FR 74815 (Nov. 30, 2015); and 86 FR 68291 (Dec. 1, 2021).

## Section 8: Privacy Risks and Mitigation

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks***

***being mitigated?***

***Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:***

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

The Avue system is used by DOJ/OARM and is critical for recruitment and managing applicant information. Privacy risks associated with this system include the compromise of Avue data via unauthorized access, disclosure of sensitive personal information, damage to the integrity of, or preventing the availability of information.

Avue duties shall be clearly delineated to decrease the risk of the potential for abuse of authorized privileges and the minimization of collusion. Information systems will enforce system access authorizations to support separation of duties. Users who pull reports that contain specific PII must have role-based access and permissions from Avue personnel who, likewise, have appropriate access to PII. Access privileges are inherited from the roles to which Avue personnel are assigned. Privileges specify the system functionality and data records to which each role has access. The rule of least privilege always applies, in that no Avue employee is provided with roles and permissions beyond the duties they must perform. In a case where multiple roles are assigned to one individual, whose position and duties cannot be separated, the user signs Rules of Behavior that explicitly note that the user is to only perform the functions of the role in which they are assigned and must not abuse the multiple roles in which they are assigned.

The following separation of duties will be implemented. Exceptions cannot be approved for regular day-to-day operations or in response to a security incident.

• An operator will not enforce authorizations within the system he/she is operating;
• A DOJ/OARM user will not approve their own access authorizations (these are performed by Avue Help Desk);
• A DOJ/OARM user will not create their own user account nor assign or approve their privileges (these are performed by Avue Help Desk);
• An admin of a system will not conduct audit/reviews of the system he/she is administering over (this is performed by a third-party assessment organization annually; OARM may review logs upon request);
• An Information Security System Officer (ISSO) will not be a system admin of any system (the Avue Senior System Security Officer is not a system admin of the Avue System); and
• No user will input information and validate the information inputted. DOJ/OARM users do not input information; this task is performed by the applicant and DOJ/OARM users validate and review the information input.

Security/security control implementation shall not be the same person conducting security reviews/audits/audit trail reviews. The following functions will be separated:

- Data collection and preparation;
- Data verification, data reconciliation, and data approval; and
- Software development and maintenance functions.

Avue is utilized by authorized OARM managers and component employees to govern the information collected in connection with all HP and SLIP applicants' application for employment at DOJ.[1] The documentation collected is only available to staff with a need-to-know and is secured by access controls. This information includes data collected as captured in Section 3.

On Avue's website, users are presented with the Avue Technologies Corporation Privacy Policy. By reading through the policy and continuing to use the website, the users consent to the collection and use of PII for DOJ/OARM requirements or for basic management functions. The website also lists out the information that is collected, the purpose of collecting the information, and how data is used legally by Avue. Additionally, users will be provided with a Privacy Act Statement that complies with the requirements of 5 U.S.C. § 552a(e)(3), and this Privacy Impact Assessment will be published, maintained, and updated as needed on the Department's Office of Privacy and Civil Liberties website.

Avue includes appropriate character limits for manual input text fields to reduce the risk of overcollection of information. Avue also employs role-based field-level security that restricts users' access to view and edit specific fields based on the principle of least privilege. Avue enforces file upload restrictions (by size, extension, malicious code, etc.) at multiple endpoints across the platform. These restrictions are tested annually as part of Avue's Third Party Assessment Organization (3PAO) assessment process, as well as confirmation tests performed by Avue SecOps staff using an anti-malware test file and files designed to test upload file size restrictions.

Decisions regarding security and privacy administrative, technical, and physical controls over the information are handled by Avue's separation of duties for Privileged and Non-Privileged user accounts. To leverage role-based access control, all system and application data is sent to an internal General Support System's centralized audit log management system for triage and review. Users of Avue connect to the AWS-hosted environment over secure VPN tunnel between the user's workstation and an OpenVPN server. SSL/TLS ensures that the data is confidential and is not tampered with. Passwords are encrypted and all weak algorithms are removed. Additionally, Avue executes Memoranda of Understanding and Interconnection Security Agreements between itself and any third party outside of its security boundary, which currently includes OPM USAJobs.

[1] OARM also provides a report to law school career services officers who can check the status of their students (with student permission) throughout the hiring process. Law school Career Services Offices (CSO) do not provision their own accounts. DOJ/OARM provides a list of individuals who should receive law school accounts to the Avue Help Desk, which then creates and assigns the correct role and permissions for the law school CSO.