United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
The Equal Employment Opportunity Application Suite

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: October 21, 2022

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (DOJ or "the Department") Equal Employment Opportunity Application Suite (EEOAS) is comprised of a commercial off the shelf (COTS) web-based application to manage, track, and report on Department EEO complaint cases. EEOAS allows DOJ to comply with federal reporting requirements. Although most of the individuals covered by EEOAS are DOJ employees, applicants seeking employment with DOJ may also file EEO complaints. Because this system contains personally identifiable information (PII) of applicants, JMD prepared this Privacy Impact Assessment.

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.

As an Executive Branch agency, DOJ is required to implement and maintain an equal employment opportunity (EEO) program. In accordance with Part 4 of HR Order 1200.1,[1] it is the policy of the Department "to provide, ensure, and promote equal opportunity in employment for all persons on the basis of merit." Additionally, DOJ management, "within every organization and at all levels will take effective actions to eliminate any internal policy, practice, or procedure which results in discrimination on the basis of race, color, religion, national origin, sex, gender identity, age, disability (physical or mental), genetic information, status as a parent, sexual orientation, marital status, political affiliation, or any other non-merit factor." The Justice Management Division (JMD), Equal Employment Opportunity Staff (EEOS), is responsible for developing Departmental policies, methods, and procedures for implementing DOJ's EEO program. Included in such a program are administrative and technological processes to manage, track, and report on EEO complaints for DOJ.

A DOJ employee or an applicant for federal employment may institute an EEO complaint if that employee or applicant believes that he/she has been discriminated against based on one or more factors including race, color, religion, national origin, sex, age, disability, protected genetic information, parental status, or reprisal. The complaint process for each case includes an informal complaint process followed by a formal complaint process. The date the formal complaint is filed is used for calculating the length of time for processing the various steps in the formal process. The formal process includes an impartial investigation completed within 180 days from the date of the formal complaint. During the investigative stage of the process, the Department has the following responsibilities: to conduct and complete the investigation; to make attempts at settlement; and to provide the complainant with a copy of the investigative file and notice of rights. Within 30 days of receipt of these materials, the complainant must request either an Equal Employment Opportunity Commission (EEOC) hearing or an immediate final agency decision from the Department.

---

[1] https://www.justice.gov/jmd/hr-order-doj-12001.

EEOAS is comprised of a COTS software package from Tyler Technologies. EEOAS is an enterprise level web-based application to manage, track, and report on EEO complaint cases. The EEOAS software allows DOJ to, among other tasks, comply with the reporting requirements of the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462) and pursuant to the Notification and Federal Employee Anti-Discrimination and Retaliation Act of 2002 (No FEAR Act), and the Elijah Cummings Federal Employee Anti-Discrimination Act.

EEOAS contains information relating to the complaint, including personally identifiable information (PII) about the complainant and other individuals referenced in the complaint file such as: name, personal address, personal email address, personal telephone number, work address, work email address, telephone number, race, gender, ethnicity, national origin, age, date of birth, place of birth, country of origin, religion, health records (including identification of mental or physical impairments), applicant information, employment status and history, employment performance rating and other information, and legal documents.

Only EEO approved staff has access to the information, which is accessible by a web browser. EEOAS data is owned and managed by the JMD EEOS, stored on DOJ servers, and used by designated EEO officials at supported Components.

Users can retrieve information by name or other personal identifier. The application is not publicly accessible, and information is only accessible from within the internal network and only to authorized users through a web browser.

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	No FEAR Act, Pub. L. No. 107-174, 116 Stat. 566 (2002); 42 U.S.C. 2000e-16; 29 U.S.C. 204, 206; 29 U.S.C. 633; 29 U.S.C. 791; 42 U.S.C. § 2000e-16(b); Section 15(b) of the Age Discrimination in Employment Act of 1967, 29 U.S.C. § 633a(b); Section 505(a)(1) of the Rehabilitation Act of 1973, 29 U.S.C. § 794a(a)(1); The Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff10; The Fair Labor Standards Act, 29 U.S.C. § 201 *et seq.*; Pregnancy Discrimination Act of 1978, Pub. L. No. 95-555, 42 U. S. C §2000e(k)

		Sections 102 and 103 of the Civil Rights Act of 1991, Pub. L. No. 102-166; Title I of the Americans with Disabilities Act of 1990, Pub. L. No. 101-336.
	Executive Order	
	Federal Regulation	29 C.F.R. § 1614.602
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	EEOC Management Directives 110 and 715

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, C	The names of complainants and individuals referenced in the complaint file, including employees, and applicants, and management officials
Date of birth or age	x	A, C	Age may be included if relevant to or referenced in the discrimination claim
Place of birth	X	A, C	National origin
Gender	x	A, C	Gender may be included if relevant to or referenced in the discrimination claim
Race, ethnicity or citizenship	x	A, C	Race or ethnicity may be included if relevant to or referenced in the discrimination claim
Religion	x	A, C	Religion may be included if relevant to or referenced in the discrimination claim
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, C	Mailing address of complainant is generally included in the complaint

(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
Personal e-mail address	x	A, C	Email address is generally included in the complaint and could include personal email address
Personal phone number	x	A, C	Phone number is generally included in the complaint and could include personal phone number
Medical records number			
Medical notes or other medical or health information	x	A, C	Could be included if relevant to or referenced in the complaint
Financial account information			
Applicant information	x	A, C	Could be included for complainants who are applicants
Education records			
Military status or other information			
Employment status, history, or similar information	x	A, C	Could be included if relevant to or referenced in the complaint
Employment performance ratings or other performance information, e.g., performance improvement plan	x	A, C	Could be included if relevant to or referenced in the complaint
Certificates			
Legal documents	x	A, C	Could be included if relevant to or referenced in the complaint
Device identifiers, e.g., mobile devices	x	A, C	Mobile phone numbers
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			

(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
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:			
- **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:			
- **User ID**	X	A	Authorized users
- **User passwords/codes**	x	A	Authorized users
- **IP address**	x	A	Authorized users
- **Date/time of access**	x	A	Authorized users
- **Queries run**	x	A	Authorized users
- **Content of files accessed/reviewed**	x	A	Authorized users
- **Contents of files**	x	A	Authorized users

(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
Other (please list the type of info and describe as completely as possible):	x	A, C	Report of Investigation Correspondence (memos, letters, emails) related to the processing of a complaint of employment discrimination. Given the purpose of EEOAS, any PII relevant and necessary to Department EEO complaints, investigations, or reports could be maintained in this system, including PII not otherwise within the above referenced categories.

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	x	Hard copy: mail/fax	x	Online	
Phone	x	Email	x		
Other (specify):					

Government sources:					
Within the Component	x	Other DOJ Components	x	Other Federal Agencies	
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		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		x	Log-in access by approved users of the application
DOJ Components	x		x	Log-in access by approved users of the application
Federal entities	X			Aggregate data (e.g., number of complaints) submitted to EEOC via an EEOC's FedSEP, which is a web-based user access only application and for the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC 462 Report). No PII is included within this report.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				

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.
Foreign governments				
Foreign entities				
Other (specify):				

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.

Individuals have been notified that EEO complaint and appeal records are covered by are EEOC/GOVT-1, Equal Employment Opportunity (EEO) in the Federal Government Complaint and Appeal Records, 81 Fed. Reg. 81116 (Nov. 17, 2016) (last published in full).

Interview witnesses (other than complainant) for employment discrimination complaint investigations maintained in EEOAS are presented with a Privacy Act Statement informing them about the collection, use, sharing or other processing of their PII.

A complainant is also presented with a Privacy Act Statement for the employment discrimination complaint interview maintained in EEOAS.

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.

A Privacy Act Notice is provided to interview witnesses (other than complainant) for employment discrimination complaint investigations. The Privacy Act (e)(3) notice informs

the witness that disclosure of the information is voluntary, but failure to provide the information could lead to potential disciplinary actions.

A Privacy Act Notice is provided to the complainant for the employment discrimination complaint interview. The Privacy Act (e)(3) notice informs the complainant that disclosure of information is voluntary, but that not providing the information could result in the complaint being delayed or canceled.

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.

Any information related to a case that is tracked in the EEOAS is included within a Report of Investigation, which is provided to a complainant.

The Privacy Act-protected records maintained within EEOAS are subject to the Privacy Act's access and amendment provisions.[2] Certain records, however, may be maintained in systems of records, such as EEOC-GOVT-1, "Equal Employment Opportunity (EEO) in the Federal Government Complaint and Appeal Records" (81 Fed. Reg. 81116 (Nov. 17, 2016), that claim exemptions to certain provisions of the Privacy Act. In such case, the applicable Privacy Act Exemptions that apply to this System of Records may limited an individual's right to access and amend the individual's records.

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).

	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): December 27, 2019 **If an ATO has not been completed, but is underway, provide status or expected completion date:**
X	**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)**

[2] 5 U.S.C. § 552a(d) (2018); *see also* 28 C.F.R. part 16 subpart D (2020) (DOJ Privacy Act access and amendment regulations).

	for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:
	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:
x	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Defense Information Systems Agency Security Technical Implementation Guide, EEOAS Configuration Scan on compliance status across multiple supported standards. Conducted on a monthly basis.
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:** Auditing logs are generated on a weekly basis. JMD EEOS and JMD OCIO are applying "Splunk" to EEOS for auditing system logs.[3]
X	**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**.
	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: All EEO counselors receive annual training on federal statutes and regulation governing employment discrimination and the processing of EEO complaints.

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?

EEOAS has a security categorization of FISMA Moderate, and DOJ has implemented all applicable privacy and security controls for a Moderate baseline. Additionally, only approved users have access to EEOAS data. Approved users can only access EEOAS with a DOJ-issued

[3] The Department's Splunk Instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

PIV card. Data in transit and at rest is encrypted on the database, therefore protecting any PII in transmission and hosted on the database. EEOAS also has its logs ingested to Splunk, which allows us to monitor role-based access. Logs are reviewed weekly by the Information System Security Officer (ISSO), and any unusual behavior is reported to the JSOC and/or Windows Team for corrective actions.

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.)

GRS 2.3; item number 110 and 111

EEOAS data on an EEO complaint of discrimination is non-permanent data. As such, data should be retained for only seven years unless an EEO complaint case is still pending resolution or unless a litigation hold is in place. Currently, data is not being disposed of in accordance with NARA guidelines because the application does not have the function to delete EEO complaint case data that might be directly or indirectly tied to another EEO complaint case that is still open. JMD EEOS and the vendor are working to modify the application to dispose of data as required.

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:

EEOC/GOVT-1, Equal Employment Opportunity (EEO) in the Federal Government Complaint and Appeal Records, 81 Fed. Reg. 81116 (Nov. 17, 2016) (last published in full).

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (July 14, 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.***

EEOAS collects information necessary to manage and track EEO complaints and comply with federal reporting requirements. EEOAS does not routinely collect information that is not relevant to tracking EEO complaints; this includes certain data types (such as Social Security Numbers) to minimize the collection of PII.

EEOAS generally maintains only personal information on DOJ employees, with only a small portion being DOJ applicants who file EEO complaints. This collection limitation minimizes the risk to individual privacy on members of the public.

Any collection of personal information creates a risk that individuals without authorization will access system information. To minimize these risks, access to EEOAS is limited to authorized DOJ users who are approved EEO officials in JMD and supported DOJ components. EEOAS can only be accessed from within the DOJ internal network. EEOAS has no interconnections with other systems. The information in EEOAS is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements.

To further minimize privacy risks, all DOJ users with access to Department networks, pursuant to Department Order, must receive an annual Cyber Security Awareness Training (CSAT) and acknowledge and agree to abide by a Rules of Behavior (ROB). The CSAT and ROB include information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII, identify potential risks and vulnerabilities associated with using DOJ-owned IT systems, provide a review of the user's role in protecting these systems, and establish guidelines to follow at work and in mobile settings to protect against attacks on IT systems. Failure to successfully complete this training and agree to the ROB can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.