Federal Bureau of Investigation

Privacy Impact Assessment
for the
[eFile & Entellitrak]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [Component to insert date of PIA approval]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The FBI's Office of Equal Employment Opportunity Affairs (OEEOA) processes employment discrimination Complaints filed by or against current or former FBI employees and applicants, as well as those contractors and detailees who are determined by FBI OGC to meet the legal definition of "employee". .[1] eFile and Entellitrak are applications used by the FBI to track these discrimination Complaints. eFile is accessible to any user with an FBINet account; Entellitrak is only accessible to OEEOA users. Both applications operate within the FBI "secret" level enclave. eFile users can submit OEEOA Complaints and monitor the status of existing Complaints. Entellitrak users can search existing OEEOA Complaints, create new OEEOA Complaints (for OEEOA Complaints submitted by postal mail, fax, or email instead of through eFile), update Complaint status, and run reports. eFile does not generate reports.

OEEOA provides Entellitrak data to the Equal Employment Opportunity Commission (EEOC) if the Complainant requests a hearing at EEOC, or to the Department of Justice (DOJ) if the Complainant requests that DOJ render a determination based solely on the written record, which includes OEEOA's Report of Investigation (ROI)[2] in addition to Entellitrak information. Also, with FBI Office of the General Counsel (OGC) approval, OEEOA provides Entellitrak data in response to formal compliance and oversight requests (e.g., requests from the Office of the Inspector General, FBI Office of Professional Responsibility, FBI Inspection Division, or FBI Human Resources Division). Lastly, OEEOA provides EEOC and DOJ with aggregated quarterly and annual reports that do not contain personally identifiable information (PII).

Section 208 of the E-Government Act of 2002, P.L. 107-347 requires that agencies conduct Privacy Impact Assessments (PIAs) on information technology systems that collect and maintain identifiable information regarding individuals, and, if practicable, to make such PIAs publicly available. Accordingly, this PIA has been conducted and will be made publicly available. As changes are made to this system, this PIA will be appropriately reviewed and revised.

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.

---

[1] The Equal Employment Opportunity Commission and federal courts require an evaluation of the work relationship between contract employees and the federal employer to determine if the contractor is essentially an employee. Factors include the employer's right to control when, where, and how the contractor performs the job; if work requires high level skills or expertise; if the employer provides necessary equipment; if the employer sets the hours of work; if the contractor is paid by the hour; and if the contractor is provided leave or other benefits.

[2] The ROI consists of relevant documentary evidence (emails, performance appraisals/plans, comparative data, application packets, policy guides and procedures, time and attendance reports, building access logs, etc.), and signed sworn statements from the Complainant, relevant supervisors, and witnesses. The ROI is drafted by an EEO Investigator, who is an FBI Supervisory Special Agent assigned to OEEOA. The ROI does not make a recommendation on the merits of the Complaint.

In order to file a Complaint concerning possible employment discrimination, users register for an eFile account via the OEEOA FBINet intranet page by providing their email address and selecting a password. After creating an account, users can logon to eFile to submit OEEOA Complaints and monitor key Entellitrak events in the processing of their Complaints. eFile users can only access their own Complaints. Key Entellitrak events are described in Appendix A to this document. eFile does not generate reports (other than audit logs as described in Section 3.1).

Entellitrak users are given an account and password by the OEEOA Master Administrator. (Roles are described in greater detail below.) After logging on, Entellitrak users are presented with a dashboard that allows them to search existing OEEOA Complaints, create new OEEOA Complaints (for OEEOA Complaints not received through eFile), update Complaint status, and run reports. Entellitrak users receive notification via Microsoft Outlook email when a Complaint is submitted through eFile. The notification does not contain details about the underlying complaint.

OEEOA Complaints are assigned/re-assigned by Entellitrak users to one of the following four Complaint Types, depending on the stage of the Complaint.

• OEEOA Contact – When Complainants contact OEEOA for information, whether in-person, by phone, by postal mail, by e-mail, by fax, or through eFile, the contact is captured as a Contact. The Complainant will be provided with materials that explain the Complaint process. A confidentiality agreement between the FBI and the complainant is also executed at this stage of the process, either via eFile when the Complaint is submitted, or during the first in-person contact, which generally occurs during the Informal Complaint stage. The confidentiality agreement is uploaded to Entellitrak.

• Informal Complaint – If the purpose of the Contact is to request an OEEOA Counselor, an EEO Supervisor converts the Complaint Type to an Informal Complaint. During the Informal Complaint process, the Complainant and the Complainant's responsible management official (RMO) are separately interviewed by the OEEOA Counselor. If a resolution is reached, the terms will be entered into Entellitrak. If no resolution is reached, the OEEOA Counselor will provide the Complainant with a Notice of Right to File a Formal Complaint.

• Formal Complaint – As discussed abovew, if the Complaint is not resolved during the Informal Complaint stage, the Complainant may complete a *Complaint of Discrimination* (Form DOJ-201A) and submit it to OEEOA by postal mail, fax, or email. (There is no option to submit the formal Complaint using eFile). Upon receipt, an OEEOA Supervisor will convert the Informal Complaint to a Formal Complaint, assign the Complaint to an OEEOA Specialist, and coordinate with an OEEOA attorney on next steps. Entellitrak tracks Formal Complaints through any subsequent appeals or civil actions.

• Class Complaint – When multiple parties join a Formal Complaint.

If a Complainant opts not to pursue their Complaint at any stage in the process, the Complaint is closed.

The Complainant may also opt to have an Informal Complaint or Formal Complaint resolved through the Alternative Dispute Resolution (ADR) process.[3]

Any user with a valid FBINet account can access eFile. eFile users can only access their own Complaints.

Only OEEOA personnel may be given access to Entellitrak. Entellitrak users are assigned role-based access, as follows:

- OEEOA Counselors can view, edit, search and run reports for their assigned Complaints.
- OEEOA Specialists can view, edit, search and run reports for all Complaints, to respond to electronic discovery and Freedom of Information Act (FOIA) requests.
- OEEOA Supervisors/Super Processors can assign and reassign Complaints to OEEOA Counselors and Specialists, create and edit Complaints, search and run reports for all Complaints, and convert Complaints (from OEEOA Contact to Informal Complaint, and from Informal Complaint to Formal Complaint).
- OEEOA ADR Managers can view, edit, search and run reports for all Complaints.
- OEEOA Attorneys , who are assigned to Complaints, can search and run reports for all Complaints;
- OEEOA Investigators can edit assigned Complaints, and search and run reports for all Complaints;
- OEEOA Master Administrator can manage user accounts and system settings.

In addition, FBI Information Technology Applications and Data Division (ITADD) personnel can manage user accounts and system settings, and also have physical access to Entellitrak and eFile computer servers.

When users logon to eFile, they are presented with a list of their existing assigned Complaints. Complaint details are accessed by selecting the hyperlink associated with the respective Complaint. Information can be retrieved from Entellitrak by any information captured in the system. Typically, information is retrieved by Case Number, Complainant Name, Mediator, RMO, Event, Basis, Issue Type, Event Date/date range, or user role.

Using eFile, Complainants manually enter information and upload supporting documentation. This information is immediately transmitted to Entellitrak, where OEEOA users retrieve the Complaint and supporting documentation, manually capture Complainant interactions and case notes, and upload relevant documents (e.g., Confidentiality Agreement, Notice of Right to File, and any documents relevant to the adjudication of the Complaint).

OEEOA provides Entellitrak data to EEOC, if the Complainant requests a hearing at EEOC, or to DOJ, if the Complainant requests that DOJ render a determination based solely on the written record,

---

[3] ADR is a term used to describe a variety of approaches to resolving EEO disputes by way of mediation. If no resolution is reached during mediation the Complainant will be able to continue through the EEO process. If the mediation is successful, the OEEO process will be concluded. ADR applied during the Informal Complaint process is known as "Informal ADR," while ADR applied during the Formal Complaint process is known as "Formal ADR," but the objective of ADR is the same, regardless of the stage at which it occurs.

which includes OEEOA's ROI in addition to Entellitrak information. Also, with FBI Office of the General Counsel (OGC) approval, OEEOA provides Entellitrak data in response to formal compliance and oversight requests (e.g., requests from the Office of the Inspector General, FBI Office of Professional Responsibility, FBI Inspection Division, FBI Human Resources Division). Lastly, OEEOA provides EEOC and DOJ with aggregated (no personally identifiable information (PII)) quarterly and annual reports.

Information is transmitted from Entellitrak via quarterly and annual statistical reports (aggregated data) and ad-hoc reports that may contain PII. Report data can be exported as Microsoft Excel files. eFile does not generate reports.

eFile and Entellitrak are interconnected with each other, but do not interconnect with any other system.

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
X	Statute	28 U.S.C. 33, Sec. 533 Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e et seq. Age Discrimination in Employment Act, 29 U.S.C. § 621 et seq. The Rehabilitation Act, 29 U.S.C § 791 et seq. Equal Pay Act, 29 U.S.C. § 206 (d)
X	Executive Order	E.O. 12333, Sec. 1.3(b)(20)(A) E.O. 12333, Sec. 1.4(h) E.O. 12333 Sec. 1.5(g) E.O. 13388 E.O. 13356
X	Federal Regulation	28 C.F.R. 0.85(a) 28 C.F.R. 0.85(d) 28 C.F.R. 0.85(l)
	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). <u>Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.</u>

eFile and Entellitrak collect, maintain, use and disseminate information about Complainants, Complaints and Complaint status/adjudication. In addition, the system collects, maintains and uses user logon and activity logs.

(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	eFile: A, B, C and D Entellitrak: A, B, C and D	Complainants, as well as FBI and non-FBI individuals involved in the Complaint, e.g., mediators, attorneys, and investigators.
Date of birth or age	X	eFile: A Entellitrak: A, B, C, and D	
Place of birth			
Gender	X	eFile: A Entellitrak: A, B, C, and D	Captured if gender is the basis of the Complaint.
Race, ethnicity or citizenship	X	eFile: A Entellitrak: A, B, C, and D	Captured if race, ethnicity or citizenship is the basis of the Complaint.
Religion	X	eFile: A Entellitrak: A, B, C, and D	Captured if religion is the basis of the Complaint.
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	eFile: A Entellitrak: A, B, C, and D	

(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
E-mail addresses (personal, work, etc.) Please describe in Comments	X	eFile: A, B, C and D Entellitrak: A, B, C and D	Complaints will include Complainant's e-mail address, and may include email addresses of non-FBI individuals involved in the Complaint, e.g., RMO, mediators, attorneys, and investigators.
Phone numbers (personal, work, etc.) Please describe in Comments	X	eFile: A, B, C and D Entellitrak: A, B, C and D	Complaints will include Complainant's phone number, and may include phone numbers of non-FBI individuals involved in the Complaint (i.e., mediators, attorneys, and investigators.)
Medical records number			
Medical notes or other medical or health information	X	eFile: A Entellitrak: A, B, C and D	Medical documentation is occasionally submitted by the Complainant as part of the Complaint.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	eFile: A Entellitrak: A, B, C and D	Complainant's job series, pay grade, and status (on-board, former employee, applicant)
Employment performance ratings or other performance information, e.g., performance improvement plan	X	eFile: A Entellitrak: A	
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(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
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	X	eFile: A Entellitrak: A	eFile and Entellitrak capture the fact that there are witnesses, but not the witness statements themselves.
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**			

(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 (specify)**
  - **Event (e.g., formal complaint filed, formal acknowledgment letter issued, formal acceptance letter issued)**
  - **Event Date (date respective event occurred)**
  - **Basis (protected class, e.g., race, sex, national origin, disability, parental status)**
  - **Issue Type (action alleged, e.g., appointment/hire, termination, time and attendance)**
  - **Complaint Type (OEEOA Contact, Informal Complaint, Formal Complaint, Class Complaint)**
  - **Case Number (unique system-generated number)**
  - **Case Status/Adjudication (EEO Contact Processing, EEO Contact Closure, PreComplaint Counseling, Informal ADR, Informal Closure, Formal Processing, Formal ADR, Investigation, Hearing, Final Decision, Appeal; Formal Closure, Civil Action)**
  - **Case Notes (free-form text field used by OEEOA)**
	X	eFile: A
		Entellitrak: A, B, C and D	

System admin/audit data:			
- **User ID**	X	eFile: A Entellitrak: A	
- **User passwords/codes**	X	eFile: A Entellitrak: A	

(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
- **IP address**			
- **Date/time of access**	X	eFile: A Entellitrak: A	
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	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):					

***** Entellitrak will contain info from the general public if the Complainant has an attorney, or if the Complainant is an applicant.

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	
DOJ Components	X			OEEOA provides aggregated data (no PII) from Entellitrak to the DOJ for quarterly and annual reporting.
Federal entities	X			OEEOA provides aggregated data (no PII) from Entellitrak to the EEOC quarterly and annual reporting.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Complainant attorneys will be provided with duplicate copies of any documents sent to the complainant, including any letters and the report of investigation.
Private sector				
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.

eFile and Entellitrak information will not be released to the public for "Open Data" purposes.

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 following Privacy Act Statement is included on the Complaint submission page of eFile.

> Privacy Act Statement
> 5 U.S.C. 552a(e)(3)
> Authority: The authority for collecting this information is 49 U.S.C. 114, and 42 U.S.C. 2000e-16(b) and (c). Purpose: This information is needed to initiate the employee web-based EEO complaints. Disclosure: Furnishing this information is voluntary; however, failure to provide it will delay electronic processing of your complaint. Routine Uses: This information may be disclosed to individuals that have a need to know the information in the performance of official duties associated with providing assistance in processing EEO complaints. This information may also be shared pursuant to Privacy Act System of Records EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002, 67 FR 49338).

The following Privacy Act Statement is included in Form DOJ-201A.

> PRIVACY ACT STATEMENT: I. AUTHORITY – The authority to collect this information is derived from 42 U.S.C. Section 2000e-16; 29 CFR Sections 1614.106 and 1614.108. 2. PURPOSE AND USE – This information will be used to document the issues and allegations of a complaint of discrimination based on race, color, sex (including sexual harassment), religion, national origin, age, disability (physical or mental), genetic information, sexual orientation, gender identity, parental status, or reprisal. The signed statement will serve as the record necessary to initiate an investigation and will become part of the complaint file during the investigation; hearing, if any; adjudication; and appeal, if one, to the Equal Employment Opportunity Commission. 3. EFFECTS OF NON-DISCLOSURE – Submission of this information is MANDATORY. Failure to furnish the information will result in the complaint being returned without action.

Notice is also provided pursuant to the JUSTICE/FBI-008, "Bureau Personnel Management System" SORN, 58 Fed. Reg. 51875, amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); JUSTICE/FBI-002, "FBI Central Records System", 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017).

In addition, the JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" SORN, 86 Fed. Reg. 37188 (July 14, 2021), is applicable to this system.

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.

OEEOA Complaints are initiated by Complainants, who control the information they provide Entellitrak, and consent to the sharing described in the relevant Section 5.1 Privacy Act statement.

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.

Complainants can monitor key Entellitrak events in the processing of their Complaint and submit amended and additional information as necessary. iComplaint users can then modify Entellitrak information accordingly. Complainants are also provided a copy of the ROI and given an opportunity to respond. Lastly, individuals may gain access to eFile and Entellitrak information via FOIA, Privacy Act, or other legal process (e.g., legal discovery).

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):** ATO is provided under the Enterprise Application Services Program (EASP), which is subject to separate privacy documentation. The most recent ATO was issued on 9/14/2021 and expires on 3/10/2023. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:** EASP currently supports approximately 8 systems, several of which provide direct support to FBI investigative activity. As such, the summary or release of POAMs would pose risks to the component. The EASP Information Systems Security Officer (ISSO) is involved in monitoring the security of systems and routinely ensures security vulnerabilities are identified and corrective action is taken as necessary to meet FBI IT security standards.
	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:

	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
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:** eFile and Entellitrak are audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. Audit logs are reviewed monthly by the EASP ISSO, using Kibana,[4] a data visualization tool. Users are subject to account suspension and referral to the Security Division (SecD) for further investigation.
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**.
X	**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:** OEEOA provides system training to eFile and Entellitrak users prior to use and as needed.

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?

The key privacy and security administrative, technical, or physical controls for minimizing privacy risks are as follows:

- Access to eFile and Entellitrak are password-protected (via Active Directory). In addition, access to Entellitrak is role-based. Entellitrak user groups are established by the OEEOA Master Administrator based on a defined need to know and a role requiring access to the data. Not all users have access to all data.
- Physical Access to the server is limited to System Administrators, who must have valid security clearances and receive privileged user training on an annual basis.
- Only the Master Administrator can make configuration changes to the system. General users do not have permission to make configuration changes.
- All access is controlled through Enterprise Security Assertion Markup Language (SAML) to support single sign-on user authentication and mitigate the potential for users to log into the system as another user.
- eFile and Entellitrak are networked-system accessible only via FBINet, a secure enclave; remote and mobile access is not applicable.

[4] Kibana is subject to review in separate privacy documentation.

- eFile and Entellitrak are audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. Audit logs are reviewed monthly by the System Administrator. Inappropriate usage is subject to account suspension and referral to SecD for further investigation. Audit logs are made available to the FBI's Enterprise Security Operations Center (ESOC).
- User accounts are disabled immediately when personnel are no longer actively employed within the program or are found to be using information inappropriately.
- Vulnerability scans are conducted quarterly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.
- Entellitrak and eFile information is encrypted at rest and in transit using Advanced Encryption Standard (AES) 256-bit encryption and/or Secure Sockets Layer (SSL)/Transport Layer Security (TLS) tunnels.[5]

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.)

The disposition of eFile and Entellitrak information is described in the National Archives and Records Administration Job Number N1-065-11-24, *i-Complaints Case Management System*. Information will be destroyed 25 years after case is closed.

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:

JUSTICE/FBI-008, "Bureau Personnel Management System" SORN, 58 Fed. Reg. 51875, amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); JUSTICE/FBI-002, "FBI Central Records System", 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017), and JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" SORN, 86 Fed. Reg. 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

[5]Secure Sockets Layer/Transport Layer Security is a security protocol providing privacy and data integrity between two communicating applications. See https://csrc.nist.gov/glossary/term/secure_sockets_layer.

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 type, quantity, and sources of information eFile and Entellitrak collect, uses and share are necessary to document and adjudicate OEEOA Complaints. The security and privacy administrative, technical and physical controls are tailored to the confidentiality, integrity and availability requirements of eFile and Entellitrak information, consistent with the system's purpose to track and facilitate the adjudication of OEEOA Complaints.

- The privacy risks associated with the collection and maintenance of eFile and Entellitrak information are overcollection of information, including information protected by the First Amendment, inaccurate information, unauthorized access, and unauthorized disclosures.
- The privacy risks associated with the access and use (sharing, reporting, etc.) of eFile and Entellitrak information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of eFile and Entellitrak information are the risks of unauthorized disclosures and loss of data.

These risks are mitigated generally by the controls set forth in Section 6.2.

The risk of overcollection of information is specifically mitigated by the Complainants themselves determining what information to provide when initiating Complaints and providing supporting and supplemental Complaint information. In addition, eFile and Entellitrak only accept data in the requested field format (e.g., numeric, alphanumeric, etc.).

The risk of inaccurate information is specifically mitigated by the Complainant's ability to review key Entellitrak events (which can be subsequently modified by Entellitrak users) and the ROI, and to request a formal hearing.

The risk of unauthorized disclosures is further mitigated by only releasing information in furtherance of adjudicating Complaints, in response to formal compliance and oversight requests (with OGC approval), or in aggregated format.

Appendix A, Key Entellitrak Events

Contact Stage:

- EEO Contact Processing – initial EEO contact is being processed
- EEO Contact Closure – EEO contact is closed

Informal Stage:

- Initial Contact – Informal process begins
- Initial Interview – EEO Counselor interviews the Complainant
- ADR Offered – ADR offered to Complainant
- ADR Accepted – Complainant agrees to participate in ADR
- Requested Extension – Counselor requested extension of informal counseling period
- Final Interview – Counselor completes final interview with complainant
- Withdrawal – Complainant withdraws case
- Settlement – Complainant and agency agree to settlement
- Notice of Final Interview and Right to File – Counseling stage completed. Complainant provided with notice of right to file a formal complaint.

Formal Stage:

- Formal Filed – Date formal complaint is received/postmarked
- Abeyance Start – Case processing paused (if the Complainant pursues mediation, or if the Complaint is pending a court ruling on class status)
- Abeyance End – Case processing resumes
- Acknowledgement Letter – Letter acknowledging receipt of formal complaint sent to Complainant
- Acceptance Letter Issued – Letter sent outlining issues accepted for investigation
- Amendment Request Received – Complainant requests to amend complaint
- Amendment Request Not Accepted – FBI denies amendment request
- Amendment Accepted – Accept amendment request, add new issues
- Additional Allegations Accepted – New issues accepted to be investigated
- Request Clarification-15-Day Inquiry Notice – Complainant sent request for more information
- Requested Extension – FBI requests 90-day extension to complete investigation
- Extension Approved – Complainant agrees to extend deadline
- 30 Day Sanitization Letter Issued – Case extended 30 days for redaction of ROI
- ROI Sent to Complainant – ROI sent after investigation is completed
- Files forwarded to Complaints Adjudication Office for a Final Agency Decision (FAD) – Complaint is sent to DOJ for a final decision after the investigation
- Complainant Request for FAD – Complainant requests FAD after investigation
- No Election by Complainant/FAD – Case sent to DOJ for final decision by default
- FAD-Merit – DOJ issues final agency decision
- Final Agency Decision-Dismissal (Procedural) – Case dismissed

- Final Agency Decision-AJs Decision – DOJ issues final decision affirming or denying administrative judge decision
- Complainant Appealed Decision – Complainant appeals DOJ decision
- Office of Federal Operations (OFO)[6] Decision Received – OFO makes a ruling on appeal
- Remanded – Complaint remanded by OFO to be accepted and investigated
- Settlement – Complainant and agency agree to settlement
- Withdrawal – Complaint withdrawn
- Civil Action Notification Received – Complainant files civil action
- Admin Closed – Case is administratively closed after decision is rendered and all case processing deadlines have passed

[6] OFO is the EEOC entity that rules on appeals of EEOC/DOJ decisions.