Privacy Impact Assessment (PIA) Template

ENTELLITRAK - EQUAL EMPLOYMENT OPPORTUNITY (ETK-EEO)
(Name of the Information System or Information Collection)

May 2024
Date

System/Collection Overview
The Entellitrak-Equal Employment Opportunity (ETK-EEO) Civil Rights application accelerator is an existing vendor operated system that allows FHFA the tools to effectively create, track, maintain, and manage EEO cases to their successful completion. ETK-EEO gives EEO caseworkers and managers the tools to guide, provide input, and report on all data elements and processes throughout each stage of the EEO case in addition to closed EEO cases. The system also allows the Agency to file legally required Equal Employment Opportunity Commission (EEOC) and Congressional reports. The database contains information regarding the names of individuals involved in an EEO case and the factors (such as race, national origin, disability, etc.) that are the basis of the case. It also contains intake forms, correspondence, investigative reports, settlement agreements, and case decisions. These documents may contain social security numbers, personal addresses and telephone numbers, and employment records including disciplinary files. FHFA is also further required to prevent and address any discrimination in the agency. This software also allows the Agency to identify trends based on EEO cases, which can assist the agency with addressing any issues related to discrimination. ETK-EEO is included in the Tyler Tech Product Suite Federal Risk and Authorization Management Program (FedRAMP) authorization package.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the System/Collection being procured or developed. The questions address all information collected, with emphasis on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information types (e.g., contact information, demographic information, employment information) are being collected, used, disseminated, or maintained in the System/Collection?	Individuals' Equal Employment Opportunity (EEO) complaints, settlements, medical records, personnel records, disciplinary records, names, addresses, phone numbers, date of birth information, Social Security numbers, age, race, national origin, sex, color, religion, genetic information. Alternative Dispute Resolution matters and harassment records may also be included.
1.2	What or who are the sources of the information provided to FHFA and included in the System/Collection?	The sources of the information are FHFA officials, applicants for employment, Office of Human Resource Management (OHRM) records, employee testimony, medical professionals, current and former employees, EEO counselors, specialists and investigators, investigative report documents, witness and/or manager affidavits, administrative judges, and employee and agency counsel.

1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The information is being used for Equal Employment Opportunity Commission (EEOC) Federal complaints and hearing processes, EEOC, Department of Justice (DOJ), Office of Personnel Management (OPM), and Congressional reporting requirements.
1.4	How is the information provided to or otherwise obtained by the System/Collection?	The externally originating information is provided through document requests as part of EEO counseling, investigations, witness interviews, EEO investigators, EEO counselors, EEO specialists, employees, and applicants. EEOC also provides documents.
1.5	Are Social Security Numbers (SSNs) being collected or used in the System/Collection? • If yes, describe in detail: 1) The business justification for collecting or using SSNs; 2) The consequences if SSNs are not collected or used; and 3) How the SSNs will be protected while in use, in transit and in storage. • If no, state "N/A" in the response section.	No. Social Security numbers are not collected; however, older personnel records that are used in EEO cases may contain the Social Security numbers of employees or applicants. When this occurs, the employee or applicant's social security number is redacted prior to placing the record in the system.

Section 2.0 Uses of the Information

The following questions delineate the use of information.

#	Question	Response
2.1	How will the information be used and for what purpose?	The information is used by FHFA to litigate EEO cases, and to provide required complaint data to the EEOC, DOJ, OPM, and Congress. The data is also used to resolve complaints, complete hearing records, respond to ad hoc, OIG, and/or FOIA requests, and for training purposes.
2.2	Describe any types of measures or processes in place to ensure that information is only used in the manner for which it was collected.	The software has security features in place that allows only authorized users within the Office of Equal Opportunity and Fairness (OEOF) access to the system. FHFA submits case information to the EEOC directly through EEOC's secure portal. When submitting the required reports, FHFA redacts case information that is not needed for reports. Also, when using any information during training scenarios, FHFA does not include PII or any other identifying details about a case.

Section 3.0 Retention

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

#	Question	Response
3.1	How long is the information retained?	Records for an individual case are destroyed or deleted seven years after the case is resolved, subject to any exceptions provided by the applicable retention schedule.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and National Archives and Records Administration (NARA)? If yes, provide the corresponding General Record Schedule (GRS) or FHFA specific Records Schedule number.	Yes. 5.3b Human Resource Record GRS 2.3, Item 111

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and the individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Is the information in this System/Collection retrieved by an individual's name or personal identifier such as an SSN or other identification? • If no, please put "no" in the Response section. • If yes, the System/Collection will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN(s) name and number or indicate that a SORN is in progress.	Yes. EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records.
4.2	How is notice about the collection of PII provided to individuals prior to the collection for the System/Collection (e.g., direct notice, Privacy Act Statement or public notice, SORN)? If notice is not provided, explain why not.	Privacy Act Statement is provided to employees on intake forms and formal complaint forms.
4.3	Is an individual's response to the request for information voluntary or mandatory?	The response to a request for information is mandatory for witnesses, Responsible Management Officials and OHRM document requests. A response is voluntary for the complainant.
4.4	What are the consequences if an individual declines to provide the information?	If the complainant fails to provide information, it may impact the ability to process their complaint or result in the dismissal of their complaint. If the Responsible Management Officials referenced in the response to Question 4.3 do not provide the required information, they can be found to have failed to cooperate with an official request and can be subject to disciplinary action.

4.5	What are the procedures that allow individuals to gain access to their information?	Individuals who file complaints receive a copy of the Counselor's report and the Report of Investigation (ROI) as part of the EEO case process. Individuals may also submit a request for access to their information to the Privacy Act Officer in accordance with FHFA's Privacy Act regulation, 12 CFR Part 1204.
4.6	What are the procedures for correcting inaccurate or erroneous information?	The investigative reports are reviewed by the employee, who can request changes with the Agency. At the hearing stage the employee can request changes to the record with the Administrative Judge. Requests to correct inaccurate or erroneous information can also be made to the Privacy Act Officer in accordance with FHFA's Privacy Act regulation, 12 CFR Part 1204.

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	Is information shared with internal office(s) or division (s)? • If yes, please identify the FHFA office(s) or division(s) and describe the information shared and for what purpose. • If no, please state "N/A" in the response section.	Yes. If a hearing is requested, the Office of General Counsel (OGC) is provided with the ROI and complaint file to defend the Agency in EEO matters. OHRM is also provided with the name of the employee for data requests from OGC. Settlement agreements are shared with OHRM and the Office of Budget and Financial Management (OBFM) for processing, as needed. The Agency Director is also made aware of the facts of high-profile cases. Management officials and witnesses are made aware of pending investigations and the alleged issues when their testimony is required for those cases.

5.2	Is information shared with external (outside FHFA) agencies, organizations, contractors, or other entities? For purposes of this Section, external organization(s) include Federal, state, and local government, and the private sector. • If yes, please identify the information shared, and for what purpose. • If no, skip to Section 6.	Yes. The EEOC is provided with complaint files and reports, which include Agency demographics, case type, complaint issues, settlement/ADR and case processing times. Congress, DOJ, EEOC and OPM also receive reports with similar information, as required by law. Federal courts may also receive the complaint file. OIG gains access to EEO information during audits and investigations. In instances of EEO claims/cases within FHFA's EEO office or the Agency Director (conflict cases), the Federal Deposition Insurance Company (FDIC) /or Consumer Financial Protection Bureau (CFPB) is provided with the claim/complaint information to handle such claims on FHFA's behalf per Memorandum of Understandings (MOUs) we have with both agencies. Any outside counsel who may be processing the case or the employee's representative will also have access to certain information.

5.3	Is the sharing of PII outside the agency compatible with the stated purpose of the original information collection? • If yes and a SORN applies, identify the applicable routine uses in the SORN listed in Question 4.1. • If no and/or a SORN does not apply, identify the legal authority that permits the sharing outside FHFA.	Yes, sharing this information outside of the agency is compatible with the original information collection. It is covered by the EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Record SORN. The routine uses identified in EEOC/GOVT-1 describe the permissible, external sharing of system PII, including but not limited to: a. To disclose pertinent information to a federal, state, or local agency or third party as may be appropriate or necessary to perform the Commission's functions under the Age Discrimination in Employment Act, Equal Pay Act, or section 304 of the Government Employee Rights Act of 1991; e. To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the EEOC becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation; and i. To disclose information to other federal agencies in accordance with Memoranda of Understanding or similar agreements between EEOC and other agencies that provide for coordination, cooperation, and confidentiality of documents in EEOC's employment discrimination enforcement efforts.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	Will FHFA Office of Inspector General (OIG) or non-FHFA personnel (e.g., contractor personnel, regulated entity personnel) have access to the System/Collection and information contained therein? • If yes, how will they gain access to the System/Collection? • If no, how will the agency control access to and use of that information? • Are there procedures or criteria documented in writing? If so, please describe.	Yes, FHFA's OEOF contractors who have specifically been authorized by the ETK-EEO system owner have access to the data. Permissions are granted based on the concept of least privilege. OEOF staff can monitor what information the contractors' access in the system and whether information is removed or downloaded. Currently, there are no written procedures.

6.2	Are there any conflicts of interest with respect to the System/Collection or information? If so, identify the conflicts of interest and describe how they are addressed.	No.
6.3	Describe the type and frequency of training that is provided to users that is specifically or generally relevant to the System/Collection.	ETK-EEO provides an online manual for system operations and has a webinar which may be accessed by system users upon request. Additionally, the systems owner Tyler Tech holds quarterly user forums designed to help users with common issues and feedback on potential enhancements and upgrades for better functionality. In addition, all FHFA employees are required to undergo Security, Privacy, and Records and Information Management (RIM) training at new employee onboarding training and annually thereafter. The training assures that users are aware of appropriate procedures regarding records and information, including PII. In addition, all FHFA users with elevated privileges receive specialized security training and role-based privacy awareness training.
6.4	Describe the technical/administrative safeguards in place to protect the data.	ETK-EEO received its initial FedRAMP Authorization on June 6, 2014. It is in the continuous monitoring phase of the FedRAMP program and FHFA reviews the status of ongoing assessments at least annually. FHFA has developed Customer Controls that describe the Agency's implementation of controls that are the responsibility of the customer agency, and not the responsibility of the vendor. This includes the implementation of single sign-on authentication, procedures for securely managing access to the system, assigning permissions based on the concept of least privilege, generating and reviewing audit logs, etc.

Section 7.0 Risk

The following questions describe the risk to the information within the System or Collection.

#	Question	Response
7.1	Given the amount and type of information collected, what are the risks to an individual's privacy associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy and describe how these risks are mitigated.	If files are accessed by inappropriate personnel or if EEO case information is obtained, sensitive data about Agency management decisions concerning disciplinary actions taken against the employee, employee performance information, and employee EEO activity may become available to those outside the EEO process. Such a breach would compromise the employee's privacy and confidentiality. To mitigate these risks, the data is stored encrypted at rest and is password protected, requiring a PIV card or password. Access is granted only to OEOF users who need access to the system for business purposes.
7.2	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There appears to be minimal, if any, risks associated with the length of time data is retained. However, if files are accessed by inappropriate personnel or if EEO case information is obtained, sensitive data about Agency management decisions, disciplinary actions, and employee EEO activity may become available to those outside OEOF who do not need to know the information. To mitigate risks that the information is exposed, the data is stored encrypted at rest and access to the system requires a PIV card or password. Access is also limited only to authorized OEOF users who process EEO cases.
7.3	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	The risks to the individual include both the loss of control of PII and the release of potentially sensitive data regarding the Agency decision/ actions in response to EEO claims outside of the EEO process. To mitigate these risks, individual data is redacted to the extent possible when submitting required reports. Also, in addition to complying with the requirements of the Privacy Act, complaint files are uploaded directly to the security EEOC portal. When FHFA disseminates any required investigation information externally, FHFA does so via the Agency's secure e-mail system, and the documents are encrypted, redacted, and password protected.