Privacy Impact Assessment
ETK-EEO

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: June 3, 2022
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Entellitrak -Equal Employment Opportunity (ETK-EEO)

Contact Point

David King
Director, Center for Civil Rights Enforcement
Office of the Assistant Secretary for Civil Rights
Contact Phone: (202) 720-8106

Reviewing Official

Tracy Haskins
ISSPM Plan ISCP Coordinator
United States Department of Agriculture
Contact Phone: (202) 720-8245

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- The component and system name are Entellitrak-Equal Employment Opportunity (ETK-EEO).
- Second sentence should be a brief description of the system and its function. ETK-EEO is a cloud-based enterprise-wide civil rights complaint tracking system
- Third sentence should explain why The PIA is being conducted to assess the privacy impact in the implantation of ETK-EEO. The Entellitrak-Equal Employment Opportunity (ETK-EEO) system provides core support for the mission of United States Department of Agriculture (USDA), Assistant Secretary for Civil Rights (ASCR) and its agency Civil Rights (CR) offices, both at the department and sub-agency levels. The ETK-EEO serves management needs of agency heads who are, by law, charged with the responsibility for agency compliance with civil rights laws and regulations. The Office of the Assistant Secretary for Civil Rights (OASCR) maintains ETK-EEO, which contains records relating to EEO complaints alleging unlawful discrimination against USDA employees or applications for employment. These records are covered by EEOC/ GOVT–1, EEO in the Federal Government Complaint and Appeal Records. The revised notice also conveys updates to the system location, categories of records, routine uses (one of which permits records to be provided to the National Archives and Records Administration), storage, safeguards, retention and disposal, system manager and address, notification procedures, records access, and contesting procedures.

- ETK-EEO is a cloud-based, FedRamp compliant, enterprise-wide civil rights complaint tracking system, consisting of a suite of applications supporting USDA and all Department agencies by tracking civil rights complaints. Additionally, ETK-EEO adheres to the regulatory reporting requirements and provides data for USDA civil rights reporting for USDA, Office of Inspector General, Government Accountability Office, and other federal entities. The employment discrimination complaints process supports enforcement of Title VII of the Civil Rights Act of 1964, the Rehabilitation Act of 1973 – Section 504, the implementing regulations at 7 CFR part 15d, the Equal Credit Opportunity Act, and any other applicable anti-discrimination statutes, rules, and regulations.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name is ETK-EEO and the Office of the Assistant Secretary for Civil Rights (OASCR) own(s) the system;
- The purpose of the ETK-EEO is to monitor and track the informal and formal Civil Rights functions which are the direct mission of OASCR.
- A general description of the information the system will contain all EEO complaint data throughout the EEO complaint process;
- Typical transactions conducted on the system include complaint intake, investigation and adjudication data
- Information sharing conducted by the program includes cloud-based networking between Tyler Technologies and USDA stakeholders including system administrators and authorized and verified account users;
- A general description of the modules and subsystems, where relevant, and their functions;
- In accordance with USDA policy DR 35[71-001], OASCR is provided legal authority to operate the ETK-EEO program.

The Entellitrak-Equal Employment Opportunity (ETK-EEO) system provides core support for the mission of United States Department of Agriculture (USDA), Assistant Secretary for Civil Rights (ASCR) and its agency Civil Rights (CR) offices, both at the department and sub-agency levels. The ETK-EEO serves management needs of agency heads who are, by law, charged with the responsibility for agency compliance with civil rights laws and regulations. The Office of the Assistant Secretary for Civil Rights (OASCR) maintains ETK-EEO, which contains records relating to EEO complaints alleging unlawful discrimination against USDA employees or applications for employment. These records are covered by EEOC/ GOVT–1, EEO in the Federal Government Complaint and Appeal Records. The revised notice also conveys updates to the system location, categories of records, routine uses (one of which permits records to be provided to the National Archives and Records Administration), storage, safeguards, retention and disposal, system manager and address, notification procedures, records access, and contesting procedures

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The system will collect, disseminate, and maintain information all informal and formal case data related to EEO complaint processing, monitoring, and tracking, including complaint contact information (name, address, phone number), complaint claims and bases, documentation supporting complaint and complaint communication (counselor's report, notice of right to file, rights and responsibilities, formal complaint, accept/dismiss letter, etc.), investigation documentation (investigation request letter, investigation plan, amendment approval/denial, report of investigation, etc.).

1.2 What are the sources of the information in the system?

The sources of information in the system are the EEO process stakeholders including agency representatives, complainants, EEO specialists and other authorized account holders.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected, used, disseminated, and maintained to track, monitor and report on the EEO operational process within the USDA.

1.4 How is the information collected?

The information is uploaded into the system by the above mentioned EEO process stakeholders.

1.5 How will the information be checked for accuracy?

The accuracy of collected information will be conducted by EEO specialists and system administrators.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authority for collection of this data is found with EEOC Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000e 29 C.F.R. Part 1614 Rehabilitation Act, 29 U.S.C. §791; Age Discrimination in Employment Act, 29 U.S.C. §621 Equal Pay Act, 29 U.S.C. § 206(d); Genetic Information Nondiscrimination Act, 42 U.S.C. §2000ff; Administrative

Dispute Resolution Act of 1996, 5 U.S.C. §571; Alternative Dispute Resolution Act of 1998, 28 U.S.C. §651; EEOC Management Directive-110 MD-715.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Secure transmission of data import/export tasks, and data migration efforts, security with a government approved encryption tool, and creation of policy and/or procedures surrounding data implementation.

Work product containing Personally Identifiable Information(PII) must be properly secure and access to this information is limited to authorized personnel. All PII incidents or violations are to be reported to COR within 1 hour ofoccurrence.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information collected will be used to monitor, track and report on the EEO activity for USDA.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The tools used to analyze data are system generated reports that are produced through the data input by authorized users and stakeholders.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

ETK EEO authorized account users, OASCR System Administrators and Tyler Technology Administrators, along with system business rules will ensure that the information is handle according to the prescribed usage. ETK-EEO is a role-based system (role-based access control is used to limit who has access to data) that follows all required security controls deemed applicable by NIST-800-53 Rev 4. Information

is protected through various levels of security. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary. Further, only authorized agency users have access to these records, access to information is provided on a need-to-know basis in order for them to perform their responsibilities, and follows the "least privilege" policy. Lastly, ETK-EEO is protected and accessed via a USDA LincPass/eAuthentication, which serves as a gateway for accessing the system.

Section 3.0 Retention

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

3.1 How long is information retained?

Data retention period will be determined by USDA record management Guidelines for seven years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, for NARA retention period of seven years. GRS Schedule 2.3 – Employee Relations Records

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There are no foreseen risks associated with the length of time data is retained as the stored data is maintained on encrypted servers and all inbound and outbound data is transmitted through secure data tunnel.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Complaint data as described in 1.1 will be shared with USDA Mission Area Civil Rights directorates, Center for Civil Rights Enforcement (CCRE) Adjudication

directorate and OGC all for the purpose of filling their specific roles and responsibilities within the EEOC complaint process.

4.2 How is the information transmitted or disclosed?

All data is maintained on encrypted servers and transmitted via secure data tunnels.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There are no foreseen risks associated with the internal sharing of information as the data is maintained on encrypted servers and all inbound and outbound data is transmitted through secure data tunnel.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information is shared externally with various Federal agencies and entities listed below:

The routine uses for this system are compatible with the purpose for which these records are collected. In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, records maintained in the system may be disclosed outside USDA for several routine uses. While these routine uses set forth do allow for disclosure outside USDA, and so have some impact on privacy of individuals, they are either necessary for carrying out the component's mission, are required by law, or benefit the subject of the records. On balance, the needs of USDA and the benefits of the individuals of these disclosures justify the minimal impact on privacy.

Such permitted routine uses include the following:

A. To the Department of Justice (DOJ) when: (a) USDA or any component thereof; or (b) any employee of USDA in his or her official capacity where the Department of Justice has agreed to represent the employee; or (c) the United States Government, is a party to litigation or has an interests in such litigation, and USDA determines that the records are both relevant and necessary to the litigation and the use of such

records by the Department of Justice is deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records.

B. To a congressional office in response to an inquiry from that Congressional office made at the written request of the individual about whom the record pertains.

C. To the United States Civil Rights Commission in response to its request for information, per 42 U.S.C. 1975a.

D. To the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management activities being conducted under 44 U.S.C. 2904 and 2906.

E. To appropriate agencies, entities, and persons when (1) USDA suspects or has confirmed that there has been a breach of the system of records; (2) USDA has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach; or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach. When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, USDA may disclose the record to the appropriate Federal, State, local, foreign, Tribal, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.

G. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the USDA or other Agency representing the USDA determines that the records are both relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding. The

following information collection (Office of Management and Budget (OMB) control number and expiration date) associated with this system has been approved by OMB pursuant to the Paperwork Reduction Act: 0579-0071, expiration date 02/28/22.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, it is covered by USDA/OASCR-1, Civil Rights Enterprise System (CRES). The following information collection (Office of Management and Budget (OMB) control number and expiration date) associated with this system has been approved by OMB pursuant to the Paperwork Reduction Act: 0579-0071.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

All data is maintained on encrypted servers and transmitted via secure data tunnels.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There are no foreseen risks associated with the external sharing of information as the data is maintained on encrypted servers and all inbound and outbound data is transmitted through secure data tunnel.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, the Civil Rights Enterprise System: USDA/OASCR-1, Civil Rights Enterprise System (CRES)

6.2 Was notice provided to the individual prior to collection of information?

Yes, As provided within the EEOC's Management Directive 110, at the initial counseling session, EEO Counselors must advise individuals in writing of their rights and responsibilities, including information pertaining to the scope of information collected in the EEO complaint process.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes, individuals may decline to provide information. However, individuals are asked to provide basic information to be used for record-keeping purposes and to determine whether the matter is covered under EEOC, EEO jurisdiction.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes, however, processing of complaint is integral to the information being uploaded into ETK-EEO

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided through the SORN and there are no foreseeable significant risk factors as EEO Counselors provide information on the process of collecting information at the onset of the Informal Complaint Process and individuals are afforded ongoing access to information throughout the Formal Complaint and Investigation Process via EEO case management personnel.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

The procedures are conveyed to the complainant through the informal process. The informal process is the agency's effort to resolve the complaint issue by offering Alternative Dispute Resolution (ADR) prior to the complaint entering into the formal process. If ADR is accepted, mediation and contact type of mediator is entered to begin the mediation process. If ADR is refused, the informal process includes: case file creation for tracking including entry of complainant contact information, complaint claims, events, requested corrective action, supporting documents, fees and case closure; engaging an EEO Counselor to create the counselor's report, acknowledgment of complaint, notice of rights and responsibilities, notice of right to file formal. If the complaint is not resolved through the informal process, the complaint is moved forward with the complete case file of collected data to the formal complaint process,

7.2 What are the procedures for correcting inaccurate or erroneous information?

All of the collected information is documented, and the complainant has the opportunity to request any modifications throughout the informal and formal complaint process.

7.3 How are individuals notified of the procedures for correcting their information?

Throughout the process the complainant is provided written instruction on how to correct any information that has been provided.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There are no foreseen risks associated with the redress of of information as the data is maintained on encrypted servers and all inbound and outbound data is transmitted through secure data tunnel

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

ETK EEO OASCR Administrators will establish authorized accounts to grant access to the system of secured data. Access will be determined and administered based on account criteria and approve access for account user verified through Linc Pass login. The list of users who have authorized access to the system is listed on the below 8.1/8.2 appendix.

8.2 Will Department contractors have access to the system?

Yes, under same criteria as listed above. A list of authorized contractors who have access to the system is listed on the below 8.1/8.2 appendix.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All authorized account users are required to train on the specifics and requirements of the ETK-EEO system and no user will be granted access without completion of the USDA Privacy/PII Information handling training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

This is a new system, certification and accreditation review is in process pending completion of the ATO/ATU.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

ETK-EEO OASCR Administrators and Tyler Technologies Administrator are charged with monitoring system and data for any misuse and to report any incident of misuse to the system owner and system manager. Each authorized user account is assigned specific access roles and limits to data access and usage that are monitored by system administrators. Accounts that are flagged for misuse are immediately locked by administrators and reported to system owner and director.

The application is hosted with Tyler Federal in a FedRAMP-Authorized environment. Tyler Federal enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards. The application utilizes role-based authentication to ensure only authorized users can access information, and they can only access the information needed to perform their duties. Authentication to the server is permitted only over secure, encrypted connections. A firewall is in place which allows only specific trusted connections to access the data. The application complies with all National Institute of Standards and Technology (NIST) standards. Physical safeguards for the data centers are detailed within the system security plan and are assessed as part of the FedRAMP assessment. Tyler Federal does not consume, process, or view the customers' data; no hard copies are made. Tyler Federal does not access customer production applications without specific approval from the system owner (possibly for troubleshooting purposes). The customer manages application- level access and accounts. Multiple layers of cryptographic mechanisms are in place. There is role-based access control within the application.

Tyler Federal performs monitoring, testing, and evaluation of our software and hosting environment. Such as:

- As a part of our continuous monitoring plan, Tyler Federal evaluates and tests a selection of controls internally on a scheduled basis.
- Assessments are conducted annually by Tyler Federal's third-party organization as part of FedRAMP continuous monitoring requirement; results are reported within the security assessment report. Additionally, MicroPact/Tyler Federal supports multiple customer assessments each year and evaluates those results
- The system production environment has multiple monitoring tools in place. Infrastructure logs are audited. Application-level audit logs can be run by the customer from the

administrative module. Tyler Federal also has a continuous monitoring plan in place, which schedules the evaluation/testing of select controls internally.

8.6 **Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?**

There are no foreseen privacy risks associated with the collection and sharing of information as the data is maintained on encrypted servers and all inbound and outbound data is transmitted through secure data tunnel.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 **What type of project is the program or system?**

ETK-EEO is a cloud-based enterprise-wide civil rights complaint tracking system, consisting of a suite of applications supporting USDA and all Department agencies by tracking civil rights complaints. Additionally, ETK-EEO adheres to the regulatory reporting requirements and provides data for USDA civil rights reporting for USDA, Office of Inspector General, Government Accountability Office, and other federal entities. The employment discrimination complaints process supports enforcement of Title VII of the Civil Rights Act of 1964, the Rehabilitation Act of 1973 – Section 504, the implementing regulations at 7 CFR part 15d, the Equal Credit Opportunity Act, and any other applicable anti-discrimination statutes, rules, and regulations.

9.2 **Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.**

N/A

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 **Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?**

Yes, however this system does not use or access any third-party websites and applications.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

This system does not use or access any third-party websites and applications.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

This system does not use or access any third-party websites and applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

This system does not use or access any third-party websites and applications.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

This system does not use or access any third-party websites and applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

This system does not use or access any third-party websites and applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

This system does not use or access any third-party websites and applications.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

This system does not use or access any third-party websites and applications.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

This system does not use or access any third-party websites and applications.

10.10 Does the system use web measurement and customization technology?

This system does not use or access any third-party websites and applications.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

This system does not use or access any third-party websites and applications.

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

This system does not use or access any third-party websites and applications.

Responsible Officials

TRACY HASKINS Digitally signed by TRACY HASKINS
Date: 2022.06.13 11:28:15 -04'00'

Tracy Haskins
ISSPM Plan ISCP Coordinator
United States Department of Agriculture

Approval Signature
Kenneth J. Baisden, Sr.

Kenneth J. Baisden Sr.
Director, Employment Investigations Division
Center for Civil Rights Enforcement
Office of the Assistant Secretary for Civil Rights

8.1/8.2 Appendix – Authorized System Access Active - Users

Administrator	Yes
Agency CR Director	Yes
Agency Specialist	Yes
CAD Manager	Yes
CAD Specialist	Yes
CAD Support Staff	Yes
Conflict Management Staff	Yes
Conflict Manager	Yes
Conflict Support Staff	Yes
ECD Manager	Yes
ECD Specialist	Yes
ECD Support Staff	Yes
EID Manager	Yes
EID Specialist	Yes
EID Support Staff	Yes
Master Administrator	Yes
Read-Only	Yes
Super Processor	Yes
Super User	Yes

All authorized users granted access to the system are USDA employees or authorized contract employees who are contracted to fulfill the same roles as listed above. In order to gain access to the system each user is required access the system via LincPass login.