



AmeriCorps Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	Name of the information system:	Equal Employment Opportunity (EEO)
1-2	System Identifier (3 letter identifier):	EEO
1-3	Unique Investment Identifier (Exhibit 53):	
1-4	Office or entity that owns the system:	Office of Diversity, Equity, Inclusion, and Accessibility, Civil Rights and Employment Branch (CRE)
1-5	Office or entity that operates the system:	AmeriCorps Office of Information Technology (OIT)
1-6	State if the system is operational or provide the expected launch date:	This new System's expected launch date is September 4, 2023
1-7	System's security categorization:	Moderate
1-8	Date of most recent Security Assessment and Authorization (SA&A) or why one is not required:	System is in the process of getting an initial ATO.
1-9	Approximate number of individuals with PII in the system:	Any AmeriCorps Federal employee or perspective federal employee who files an EEO complaint.



250 E Street SW
Washington, D.C. 20525
202-606-5000/ 800-942-2677



3- SIGNATURES (ORIGINAL MAINTAINED BY CHIEF PRIVACY OFFICER)			
	Role	*Signature*	*Date*
3-1	Information System Owner:		
3-2	Office of General Counsel:		
3-3	Chief Privacy Officer:		
3-4	Chief Information Security Officer:		
3-5	Senior Agency Official for Privacy:		

4- PIA HISTORY	
4-1	State whether this is the first PIA for the system or an update to a signed PIA.
	First PIA for this system.
4-2	If this is an update, describe any major system changes since the last PIA. If this is the first time a PIA is being completed, write <u>Not Applicable</u>.
	Not Applicable
4-3 A	State whether this is the annual review of PIA.
	No
4-3 B	Describe any changes to the system, data activity, policies, procedures, any interrelating component and process, vendor, 3rd parties, contracts and any required controls since last PIA.
	Not Applicable
4-3 C	Describe objects and results of audit or tests (continuous monitoring).
	The system will be assessed on August 2023. The Cloud Service Provider is Fed Ramp authorized and provides most of the security controls. They perform continuous monitoring and scan the system monthly.
4-3 D	Certify and state “Completion of Review” if no change occurs.
	This is the first PIA for this system.
4-4	If the system is being retired, state whether a decommission plan is completed and attach a copy.
	Not Applicable

5- SYSTEM PURPOSE	
5-1	Describe Purpose of the System (or program, product, service)
	The Equal Employment Opportunity (EEO) system is an enterprise level Commercial Off-the-Shelf product that AmeriCorps procures from Tyler



	<p>Technologies as a turnkey project. EEO is a web-based, enterprise application developed specifically to manage the Equal Employment Opportunity complaints and Alternative Dispute Resolution (ADR) activities and generate the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaint -EEOC Form 462 which summarizes the details of each Equal Employment Opportunity complaint processed by a Federal agency between October 1st of one year through September 30th of the next year. The Civil Rights and Employment Branch (CRE) of AmeriCorps uses EEO system to collect, track, manage, process, and report on information regarding Equal Employment Opportunity complaint cases filed by AmeriCorps employees and prospective employees.</p> <p>The system is accessed via a website hosted by Tyler Technologies: https://eoo-ameriCorps-prod.entellitrak.com</p>
--	--

6- INVENTORY OF PII

6-1	<p>Provide a list of all the PII included in the system.</p> <p>EEO system collects PII for case management, business process management, and data tracking for AmeriCorps. The types of PII stored in the EEO system of AmeriCorps includes: Employee Identification Number, Personal Mobile Number, Case files, Disability Information, Name, Date of Birth (DOB), Country of Birth, Home Address, Personal Email Address, Gender, Ethnicity, Zip Code, Sexual Orientation, Business Phone or Fax Number, Business E-mail Address, Race, Nationality, Marital Status, Religion, Home Phone or Fax Number, and Employment Information.</p> <p>The main section of the Home Tab of the application menu includes Case Number, Type, Status, Complainant, Case Manager, Case Processor, Initial Contact, Filed Date, Last Event, Last Event Date, Age, Days Left.</p> <p>The complaint screen includes retrievable information such as Personal Information (First Name, Last Name, DOB, UID, EIN, Race, Gender), Employment Information (Pay Plan, Grade, Step, Series, Employee Type, Occupation, Bargaining Unit), Contact Information (Email, Alt Email, Home Phone, Work Phone, Personal Cell Phone, Work Cell Phone, Preferred Contact Method)</p>
------------	--

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM

7-1	<p>Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.</p>
------------	--



	The system has information collected from both AmeriCorps employees and prospective employee (i.e., those going through the interview and hiring process avail themselves of the EEO Process and thus be a part of this system).

8- INFORMATION IN THE SYSTEM

8-1 A	For each category of individuals discussed above: Describe the information (not just PII) collected about that category and how the information is used.
	<p>The individual filing the complaint would provide their PII which would be used to track the Equal Employment Opportunity (EEO) cases.</p> <p>The CRE staff might collect information from the witnesses if necessary.</p> <p>The system will be audited, and the audit logs will include who accessed the system, who has created, modified, or deleted information, and privileged granted to the user. A limited number of employees will be authorized to access the system and review audit logs for information security management purpose.</p>
8-1 B	State whether the system derives new data, or creates previously unavailable data, about an individual via aggregation of information or other means. Explain why, how it is related to the purpose of the system, how it is used and with whom it is shared.
	Not Applicable. The system does not derive new data, or creates previously unavailable data, about an individual via aggregation of information or other means.
8-1 C	If the system uses commercial or publicly available data, explain why, how it is related to the purpose of the system, and how it is used.
	Not Applicable
8-1 D	Describe any application of PII redaction, mask, anonymization or elimination.
	There is no PII redaction in the system. Only a limited number of users are authorized to access the system. All data in the system is protected through encryption.
8-1 E	Describe any design that is used to enhance privacy protection.
	Access to data that exists in the system is only granted to users who have the need to know by the system owner. There are specific roles defined in the system and each role can only have access to data via an approval and authorization process. A user will be granted access to the system through Single Sign On (SSO) which utilizes the user's PIV card and PIN number for authentication.

9- COLLECTIONS OF PII INTO THE SYSTEM

9-1	Describe for each source of PII in the system:
------------	---



	<p>1. The source. 2. What comes from that source. 3. How the PII enters the system.</p> <p>The source of PII includes AmeriCorps Federal employees or potential federal employees who file an EEO complaint. The employees in the Office of Diversity, Equity, Inclusion, and Accessibility might collect witness information if necessary.</p> <p>The information collected from the complainant includes First Name, Last Name, DOB, UID, EIN, Race, Gender, Employment Information such as Pay Plan, Grade, Step, Series, Employee Type, Occupation, Bargaining Unit, and Contact Information such as Email, Alt Email, Home Phone, Work Phone, Personal Cell Phone, Work Cell Phone, Preferred Contact Method.</p> <p>The information collected from the witness includes name, position, and potential relation in terms of work or member/volunteer status. There may potentially be demographics on witnesses depending upon the type of allegation being made in the complaint.</p> <p>The CRE staff member would manually enter this information into the system.</p>
<p>9-2</p>	<p>If any PII comes directly from the individual, describe the privacy controls in place. If all PII comes from a secondary source, write <u>Not Applicable</u>.</p> <p>The PII is provided directly by the individuals who file EEO complaint. Office of Diversity, Equity, Inclusion, and Accessibility (CRE) staff may collect information from the complainant and/or witnesses. CRE employees would enter this information manually into the system.</p> <p>The CRE staff conduct the complainant intake by following standard procedures. An individual would contact the CRE first regarding a claim of employment discrimination they would like to make. During the intake process the individual is told by an EEO Specialist how the information the individual provided would be used and handled. The EEO specialist would ensure that the claim is made with one of the jurisdictional bases under Title VI and limit the flow of information to only those who it is necessary or asked to divulge information to by the complainant. The information written in Counselor's Reports to limited to what is necessary to help frame the claim or that is sought to obtain the resolution the complainant is seeking.</p>



	<p>Only CRE EEO specialists are authorized to collect and enter the information collected via the claim intake process into the system which has secured connection and encryption controls in place to protect the PII at rest and in transit. The access into the system is secured by MFA and VPN. A connection to the system occurs through FIPS 140-2 compliant TLS connection utilizing 256-bit AES encryption.</p>
9-3	<p>If PII about an individual comes from a source other than the individual, describe:</p> <ul style="list-style-type: none"> a. Why the PII is collected from the secondary source. b. Why the PII from the secondary source is sufficiently accurate. c. If/how the individual is aware that the secondary source will provide their PII. <p>If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.</p>
	Not Applicable
9-4	<p>If any collections into the system are subject to the Paperwork Reduction Act (PRA), identify the Office of Management and Budget (OMB) Control Number for the collection and effective date. If the system does not implicate the PRA, write <u>Not Applicable</u>.</p>
	Not Applicable
9-5	<p>If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.</p>
	Not Applicable

10- SYSTEM ACCESS	
10-1	<p>Separately describe each category of individuals who can access the system along with:</p> <ul style="list-style-type: none"> a. What PII they can access (all or what subset). b. Why they need that level of access. c. How they would request and receive that access. d. How their access is reduced or eliminated when no longer necessary. e. Identify policies and procedure outlining roles and responsibilities and auditing processes.
	<p>Access to the system is controlled based on need-to-know and least privilege principles per the requirement for different roles.</p> <p>The staff members of the Office of Diversity, Equity, Inclusion, and Accessibility (CRE) will intake the case and manually enter the information into the system.</p>



	<p>The Director and one other authorized user will have Master Administrator’s privileges and they will have access to all PII in the system. Their access will be terminated when they leave their position in the organization. Their roles and responsibilities and auditing process are detailed in the system security plan.</p> <p>Case manager is a role that will be able to view all the PII on individual cases assigned to them. Case managers need this level of access to manage their cases. The Master Administrator will approve and authorize their access to the system as appropriate for them to complete their job. Their access will be eliminated as soon as it is no longer required. Their roles and responsibilities and auditing process are detailed in the system security plan.</p> <p>EEO does not have an internal policy that requires identifying roles and responsibilities. This would fall under the purview of the Civil Rights Director who will assign EEO specialists and CRE Branch personnel to a role within the system.</p> <p>The PII information both user groups can view include information such as Personal Information (First Name, Last Name, DOB, UID, EIN, Race, Gender), Employment Information (Pay Plan, Grade, Step, Series, Employee Type, Occupation, Bargaining Unit), Contact Information (Email, Alt Email, Home Phone, Work Phone, Personal Cell Phone, and Work Cell Phone). The access this information will be granted and terminated by the Director. Termination will happen the same day when a user no longer needs access.</p>
--	---

11- PII SHARING

<p>11-1</p>	<p>Separately describe each entity that receives PII from the system and:</p> <ol style="list-style-type: none"> a. What PII is shared. b. Why PII is shared (<i>specify the purpose</i>) c. How the PII is shared (what means/medium). d. The privacy controls to protect the PII while in transit. e. The privacy controls to protect the PII once received. f. PII sharing agreements (<i>describe if the agreement specifies the scope of the information sharing, parties of agreement and the duration of the agreement</i>) g. Describe security and privacy clauses and audit clauses in the agreement or vendor (including third party vendors) contract. <p>If PII is not shared outside the system, write <u>Not Applicable</u>.</p>
	<p>The EEO system does not directly share any information with any system. If the complainant files an appeal to the Office of General Counsel or EEOC will initiate a request for the complainant's case file. The case manager in EEO will download the file and upload it to a secured link provided by OGC or EEOC.</p>



12- PRIVACY ACT REQUIREMENTS

12-1	<p>If the system creates one or more systems of records under the Privacy Act of 1974:</p> <ul style="list-style-type: none"> a. Describe the retrieval that creates each system of records. b. State which authorities authorize each system of records. c. State which SORNs apply to each system of records. <p>If the system does not create a system of records, write <u>Not Applicable</u>.</p>
	<p>EEO records can be retrieved by complainant name and case number.</p> <p>EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeals Records.</p> <ul style="list-style-type: none"> • 42 U.S.C. 2000e-16(b) Discriminatory practices prohibited and (c); 29 U.S.C. 204(f) Administrative and 206(d) Minimum wage; 29 U.S.C. 633(a) Nondiscrimination on account of age in Federal Government employment.; 29 U.S.C. 791 Employment of individual with disabilities; Reorg. Plan No. 1 of 1978, 43 FR 19607 (May 9, 1978); Exec. Order No. 12106, 44 FR 1053 (Jan. 3, 1979). <p>OPM-GOV 1 General Personnel Records</p> <ul style="list-style-type: none"> • 5 U.S.C. 1302 Regulations, 2951, 3301 Civil Service, 3372 General Provisions, 4118 Regulations, 8347 Administrative regulations, and Executive Orders 9397, as amended by 13478, 9830, and 12107. • Executive Order (E.O.) 13478, Amendment to Executive Order 9397 (E.O. that established the use of SSNs) Relating to Federal Agency Use of Social Security Numbers removed a requirement for agencies to use SSNs as individuals' unique identifiers.

13- SAFEGUARDS

13-1	<p>Describe the data processing environments and the technical, physical, and administrative safeguards (including vendors') that protect the PII in the system.</p>
	<p>The EEO system is safeguarded through multiple layers of controls to protect the PII of the system.</p> <p>Administratively, all users must sign an AmeriCorps Privileged User Rules of Behavior and receive privacy and security training annually, which is documented as a performance metric monitored by AmeriCorps to ensure adequate information security and privacy compliance posture is maintained. All AmeriCorps employees are required to go through annual security and privacy training. The employees of the CRE are required to receive training on how to use the EEO system and can only be authorized by the director to access the system per the requirements of role</p>



	<p>based on need-to-know and least privilege principles. The CRE follows standard process to intake the claim, only collect information that is necessary and would inform the individuals of the uses of information at the point of collection.</p> <p>The PII entered into the system and all the data in the system are securely protected. All data in transit and at rest are encrypted and only accessed using SSL-based VPN with AES-256 encryption. Data Backups are encrypted using FIPS140-2 algorithms via Electronic File System (EFS), and VPN access is regulated using an SSL-based VPN with AES-256 encryption. The audit log is configured per standard configuration policy and is reviewed regularly. The record retention schedule is identified. The system owner will coordinate the record retention and disposition to ensure it is appropriately handled.</p> <p>The vendor Tyler Federal houses AmeriCorps data and takes full responsibility for physical safeguards needed to protect the data, including having system level breach response plan to properly handle and report breach to AmeriCorps. Tyler Federal’s software is FedRAMP approved, and an independent 3rd party assessment is conducted on an annual basis to ensure they are meeting NIST and Federal requirements.</p>
13-2	Describe the technical, physical, and administrative measures that protect PII if the system is being retired.
	Not Applicable
13-3	State if a system security plan and privacy plan is completed and the date of control verification.
	System is in the process of getting an initial ATO and is about to go through the full assessment process. The system security plan and privacy plan are currently in development and has not been completed yet.

14- DATA ACCURACY, ACCESS, AMENDMENT, AND CONTROL	
14-1	Describe the steps taken to ensure PII is sufficiently accurate, relevant, current, and complete and the assurance procedure.
	The PII is collected from one of five employees in the CRE to track EEO cases at AmeriCorps. The PII is collected from the individual with an EEO case and considered accurate.
14-2	Describe how an individual could view, correct, update, or ask to amend their PII.
	The complainant does not have direct access to the system; however, they can request to view, correct, update, or amend their records by calling or meeting with their case manager in the CRE.



14-3	Describe how an individual could control what PII about themselves is included in the system or how it is used. Also describe how those decisions could affect the individual.
	Individuals control what information they would provide to the EEO specialist in the intake process. It is a voluntary process.
14-4	State if PII handling processes apply automation technology for decision making and describe the measures taken to eliminate risk to privacy interests.
	No automation technology is used.

15- DATA RETENTION AND DESTRUCTION

15-1	Identify the National Archives and Records Administration (NARA) provided retention schedule for the system and provide a summary of that schedule.
	The PII is maintained in the system until AmeriCorps removes the PII from the system. AmeriCorps will retain the data in accordance with the AmeriCorps data retention policy. Tyler Tech maintains backups of AmeriCorps data stored in the systems and retains those backups based on the Media Retention Policy. Data will be destroyed 7 years after resolution of case, but longer retention is authorized if required for business use. Disposition authority: DAA-GRS-2018-0002-0012 and DAA-GRS-2018-0002-0013.
15-1	Identify the role and process to coordinate with the parties involved the record retention and disposition.
	The System Owner and Civil Rights Director will coordinate record retention.

16- SOCIAL SECURITY NUMBERS (SSNs)

16-1	If the system collects truncated or full social security numbers (SSNs): a. Explain why the SSNs are required. b. Provide the legal authority for the usage of the SSNs. c. Describe any plans to reduce the number of SSNs. If the system does not collect any part of an SSN, write <u>Not Applicable</u>.
	Not Applicable

17- WEBSITES

17-1	If the system includes a website which is available to individuals apart from AmeriCorps personnel and contractors, discuss how it meets all AmeriCorps and Federal privacy requirements. If the system does not include a website, write <u>Not Applicable</u>.
------	---



	Tyler Technologies website complies with all NIST requirements and governmental regulations. The website displays a privacy policy and notifies users they are entering the EEO site.
--	---

18- OTHER PRIVACY RISKS	
18-1	Discuss any other system privacy risks or write <u>Not Applicable</u>.
	Not Applicable