AmeriCorps
Privacy Impact Assessment (PIA)

1- GENERAL SYSTEM INFORMATION		
1-1	**Name of the information system:**	Civil Rights Interface (CRI)
1-2	**System Identifier (3 letter identifier):**	CRI
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:**	Expected launch date is Q4 2024
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:**	Approximately 700 based upon roughly 100 cases per year, with a retention period of seven (7) years.

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 Not Applicable.**
	Not Applicable.
4-3 A	**State whether this is the annual review of PIA.**
	Not Applicable. This is the initial PIA.
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).**
	Not Applicable.
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 Tyler Civil Rights Interface (CRI) application provides a solution for managing every part of Title VI discrimination complaints from intake to resolution while ensuring the interests of all parties are protected. The application is a Commercial Off-the-Shelf (COTS) turnkey product built on Tyler's Case Management Development Platform, powered by Entellitrak®. The features of CRI allow users to process complaints in less time, reduce investigation costs, automate workflows, connect information from multiple sources, and reduce physical paperwork. The application also provides visibility and access to all stakeholders via a secure, web-based interface. AmeriCorps uses CRI to process complaints of Title VI protected discrimination and retaliation, as well as manage correspondence, emails, and documents and the complaint activities through the entire workflow. When the system starts to operate, the recipients (service members, volunteers, and grantees) of AmeriCorps programs, services, and benefits will be able to use CRI to either inquire about or file a Title VI discrimination complaint. Those in need of accessing the system to file a complaint can log onto the web-based portal and begin their inquiry. After an individual enters and submits their basic contact information, the system will send a message to inform the CRE intake staff that an inquiry has been placed. The system will generate an automatic email that is sent to all parties informing them of an individual's use and registration. This email may also contain the initial intake information sheet required to be completed by the complainant. From there, CRE staff will contact the individual and explain the process, using CRI as an intermediary to collect and receive necessary documentation or files that the complainant believes are necessary for their case. After the counseling period, the counselor will upload the Counselor's report and send notification that a counseling has been completed. This manual step will also notify the individual of their right to file a formal complaint. If the individual chooses to file a formal complaint, the system will continue to act as the intermediary for documentation and formal notifications between the complainant and the investigator. Once the investigation is complete, the investigator will notify the complainant of the completion of the investigation through CRI.

6- INVENTORY OF PII	
6-1	**Provide a list of all the PII included in the system.**
	The CRI system collects PII for AmeriCorps' Title VI complaint process. The types of PII stored in the CRI system include: name, alias, home address, zip code, date of birth, personal and business mobile number, home/business phone or fax number, personal and business email address, spouse information, country of birth,

		employment information, race, gender, ethnicity, nationality, marital status, religion/religion preference, children information, sexual orientation, file/case ID number, civil/criminal history information/police record, case files, personnel files, health information, academic and professional background information, mental health information, disability information, and education information.

7- CATEGORIES OF INDIVIDUALS IN THE SYSTEM		
7-1	**Describe the categories of individuals whose PII is in the system and state approximately how many individuals are in each category.**	
		The system covers individuals who have filed informal or formal complaints with, or against, AmeriCorps, including any recipient of services, programs, or benefits from AmeriCorps or one of its programs. Individuals who may file informal or formal complains include AmeriCorps members, applicants, or trainees for volunteer or service status, as well as employees of a grantee or program beneficiary. To file a case, an individual will ultimately provide their contact information and all pertinent details of the violation being reported (*i.e.*, individuals involved, date, time, location, and any details the person filing the complaint deems relevant which might include PII of other individuals such as witnesses). Collectively there will be approximately 700 total people with PII in the CRI system. The number of individuals in each category might vary drastically depending on the number and context of cases filed.

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.**	
		The individual filing the complaint would provide all pertinent details of the civil rights violation(s) (who, when, what, where, etc.), as well as their relevant PII (*i.e.*, name and contact information). This information is used to create and track the case in the CRI system. The CRI staff might collect these complain details and contact information from witnesses if necessary and available. The system will be audited, and the audit logs will include who accessed, created, modified, or deleted information, and privileges 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.

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 create 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. All data in the system is protected through encryption. Only a limited number of users in the CRE office will be authorized to view case data entered into the CRI system.
8-1 E	**Describe any design that is used to enhance privacy protection.**
	Users gain access to the system and certain data based upon a user having a need to know, which is evaluated and determined 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. An AmeriCorps 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:** **1. The source.** **2. What comes from that source.** **3. How the PII enters the system.**
	The source of PII includes individuals who file a complaint in the system or individuals from who CRE staff collect relevant information about the complaint, such as witnesses. The information collected from complainants includes first name, last name, DOB, race, gender, employment information, and contact information (*i.e.*, email, alternate email, home phone, personal cell phone, work cell phone, preferred contact method).

		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. CRE staff member would manually enter this information into the system.
9-2	**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>.**	
		The PII is provided directly by the individuals who file a civil rights complaint, and/or CRE staff who may collect information from the complainant and/or witnesses. Both the individuals filing a complaint and the office of CRE can enter information into the system manually. The CRI website landing page will display a Privacy Act Statement and a banner notifying users they are entering the Civil Rights site. The information written in the CRI system is limited to what is necessary to help frame the claim or that is sought to obtain the resolution the complainant is seeking. This will minimize the PII entered into the system to what is necessary. The employees of the CRE office are required to receive training on how to use the CRI system and can only be authorized by the CRE director to access the system per the requirements of role-based access on need-to-know and least privilege principles. The CRI application includes a set of pre-defined roles for users of the system. The CR Product Administrator may add or modify these roles, as well as further configure the specific permissions assigned to them. Roles are assigned to users upon account creation and come with an array of permissions associated with the user's security level. The system is configured with the following roles: • CR Product Administrator • Case Coordinator • Investigator • eFiler There are two categories of assignable permissions: System and Data. Upon role creation, applicable permissions are assigned using the following procedures: **System permissions** grant users access to major functional areas of the application including the management of tracked items, report generation, and search. For each system permission that is granted to a user, a tab will appear in the navigation bar. These tabs include the Tracking Inbox and Search.

		Data permissions allow the user to manipulate and maintain data pertaining to the tracked items that have been assigned to the user. These capabilities include create, modify, delete, search, and assign. Access can be granted or denied for each data element in the system. Secured connection and encryption controls are in place to protect the PII at rest and in transit. Access into the system is secured by Multi-Factor Authentication (MFA) and Virtual Private Network (VPN). A connection to the system occurs through FIPS 140-2 compliant TLS connection utilizing 256-bit AES encryption.
9-3	**If PII about an individual comes from a source other than the individual, describe:** **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.** **If all PII about an individual comes directly from the individual, write <u>Not Applicable</u>.**	
		Not Applicable.
9-4	**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>.**	
		Not Applicable.
9-5	**If any collections into the system are subject to an agreement, describe those agreements. If no agreements are relevant, write <u>Not Applicable</u>.**	
		Not Applicable.

10- SYSTEM ACCESS		
10-1	**Separately describe each category of individuals who can access the system along with:** **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.**	
		Access to the system is controlled based on need-to-know and least privilege principles, per the requirement for different roles.

		The CRE Director and one other authorized user in the CRE office 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. Case manager 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. Complainants will have a general user role, and only be able to access their individual information in the system. The PII that the master administrators and case managers can view include information such as personal information (*i.e.*, first name, last name, DOB, race, gender), employment information (*i.e.*, pay plan, grade, series, employee type, occupation, bargaining unit), contact information (i.e., email, alternative email, home phone, work phone, personal cell phone, work cell phone). The CRI application includes a set of pre-defined roles for users of the system. The CR Product Administrator may add or modify these roles, as well as further configure the specific permissions assigned to them. Roles are assigned to users upon account creation and come with an array of permissions associated with the user's security level. Upon role creation, applicable permissions are assigned using the system permissions and data permission procedures. The access to the information in the system can only be approved and terminated by the CRE Director. Termination will happen the same day when a user no longer needs access.

11- PII SHARING	
11-1	**Separately describe each entity that receives PII from the system and:** **a. What PII is shared.** **b. Why PII is shared.** **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.** **g. Describe security and privacy clauses and audit clauses in the agreement or vendor (including third party vendors) contract.**

	If PII is not shared outside the system, write <u>Not Applicable</u>.	
		The CRI system does not directly share any information with any system.

12- PRIVACY ACT REQUIREMENTS		
12-1	**If the system creates one or more systems of records under the Privacy Act of 1974:** **a. Describe the retrieval that creates each system of records.** **b. State which authorities authorize each system of records.** **c. State which system of records notices (SORNs) apply to each system of records.** **If the system does not create a system of records, write <u>Not Applicable</u>.**	
		CRI records can be retrieved by complaint name and case number. The system is covered by CNCS-10-CEO-CRCM-Civil Right Case Management System of Records Notice [89 Fed. Reg. 33,336].

13- SAFEGUARDS		
13-1	**Describe the data processing environments and the technical, physical, and administrative safeguards (including vendors') that protect the PII in the system.**	
		The CRI system is safeguarded through multiple layers of controls to protect PII. Administratively, all AmeriCorps employees and contractors must sign an AmeriCorps Privileged User Rules of Behavior (ROB) 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 and contractors are required to go through annual security and privacy training. CRE employees are required to receive training on how to use the CRI system and can only be authorized by the director to access the system per the requirements of role-based access on need-to-know and least privilege principles. The PII entered in 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.

		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 third-party assessment is conducted on an annual basis to ensure the system meets federal requirements.
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.**	
		The CRI 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 the individual filing a CRI complaint and considered accurate.
14-2	**Describe how an individual could view, correct, update, or ask to amend their PII.**	
		The complainant will set up an account to file their complaint and can log back into the system to update information that changes (*i.e.*, address, license, phone number etc.).
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 provide in the CRI system when filing a complaint. 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. The records are temporary, and the records will be destroyed 7 years after resolution of case, but longer retention is authorized if required for business use. Disposition authority: General Records Schedule (GRS) 2.3.110 & 2.3.111 – EEO discrimination complaint case files [disposition authorities: 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 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>.**	
		The CRI website is not currently live but will be specific to AmeriCorps when created. The website will comply with all National Institute of Standards and Technology (NIST) requirements and governmental regulations. The home page of the website will display a privacy policy and Privacy Act Statement and a banner notifying users they are entering the Civil Rights site.

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