U.S. DEPARTMENT OF LABOR

Office of the Civil Right Center (CRC)

COMPLAINTS TRACKING AND REPORTING SYSTEM (CTRS)

PRIVACY IMPACT ASSESSMENT

VERSION 1.9

3/30/2023

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
12/18/17	CTRS PIA v1.6	DSAM	Review and Update
12/17/18	CTRS PIA v1.7	DSAM	Review and Update
11/27/20	CTRS PIA v1.8	DSAM	Review and Update
3/30/2023	CTRS PIA v1.9	DSAM	Review and Update

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
12/18/17	1.6	Privacy Team
12/17/18	1.7	Privacy Team
11/27/20	1.8	Privacy Team
3/30/2023	1.9	Privacy Team

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

The Complaints Tracking and Reporting System (CTRS System) is owned by the Office of the Assistant Secretary for Administration and Management (OASAM), Civil Rights Center (CRC). The CTRS System records and tracks discrimination complaints filed by Department of Labor (DOL) employees, members of the public who have applied for employment with DOL or members of the public who are either employed with or receive benefits from an entity that is funded by DOL. The mission of CTRS System is to track the filing, processing, timeliness and closure of Equal Employment Opportunity (EEO) and Equal Opportunity (EO) complaints filed with CRC. CTRS System provides the CRC staff with standardization of its processes and centralization of its data to significantly improve the collection, management and reporting capabilities of the organization. Components of the CTRS System capture discrimination complaints from members of the public who are either employed with or receive benefits identified above. Components of the CTRS System capture discrimination complaints from DOL employees and individuals applying for employment with DOL. CTRS System provides a national view of the level of service CRC is providing to its constituents. The information processed includes personally identifiable information (PII) in the form of names, business and home addresses, business, home and cell telephone numbers, business and personal email addresses, the EEO Complainant's race, color, religion, national origin, sex, disability, citizenship, reprisal/retaliation, genetic information, status as a parent, political affiliation, wages, harassment allegations, medical information, date of birth, device identifiers, and the alleged discriminatory action(s) that precipitated the complaint.
CTRS System features three different types of users and one role. The classifications are as follows:

• Users are permitted to access CTRS System to view records.
• Managers are permitted to access CTRS System to view records and update records (i.e., add and modify records)
• Administrators are given administrative rights to add, modify, and delete system data.

Investigators for CTRS System are DOL employees that conduct Equal Employment Opportunity (EEO) and EO investigations into issues that have been accepted. It is following the investigation that a determination is made as to whether discrimination has occurred.
CTRS System collects personal information (either on paper and/or within the system); the following laws and internal policies are cited: the Privacy Act of 1974, Office of Management and Budget (OMB) Circular A-130, and OMB M-99-18, "Privacy Policies on Federal Web Sites". Due to the collection of personal data, any disclosure of the system data to anyone who does have a need to know the data would constitute an unwarranted invasion of personal privacy. The loss, misuse, or unauthorized access or modification of this data could lead to identity theft and fraudulent activity.

1.2 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, or technology being developed.

Specify whether the System collects personally identifiable information (PII) on Department of Labor (DOL) employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

CTRS collects information on Military Service Members and Veterans of The United States of America. However, it does store or maintain any separate documents related to the case to SharePoint. The VETS Case Management System (CTRS) provides the claim intake and case processing for violation complaints filed by Military Service Members and Veterans of The United States of America

- From whom is information to be collected?

The CTRS System collects information about DOL employees and members of the public who have applied for employment with DOL or members of the public who are either employed with or receive benefits from an entity that is funded by DOL.

- Why is the information being collected?

The information is being collected in the CTRS System in order to track and report relevant information regarding EEO complaints filed with the CRC for processing (including EEO counseling, formal EEO investigations, CRC Final Agency Decisions and EEOC hearings) and EO Additionally, in accordance with the Elijah Cummings Federal Employee Antidiscrimination Act of 2020, the Department is required to have a tracking system for EEO complaints filed with CRC, from initial processing until final resolution or adjudication.

- What is the PII being collected, used, disseminated, or maintained?

Individual's name, business, and home address, telephone number, email address, race, color, religion, national origin, sex, disability, political affiliation, citizenship, reprisal/retaliation, national origin, genetic information, status as a parent, political affiliation, wages, harassment, medical information, date of birth, device identifiers, and the reason that precipitated the complaint

- How is the PII collected?

  PII data (for complainants) is initially collected via in-person meetings, telephone, email, fax, and/or paper forms or by emails and later entered into the CTRS System by the CRC staff.

- How will the information collected from individuals or derived from the system be checked for accuracy?

PII data (for complainants) is initially collected via in-person meetings, telephone, email, fax, and/or paper forms or by emails and later entered into the CTRS System by the CRC staff. Automated forms ensure appropriate field accuracy (e.g., numbers cannot be filled in for fields requiring letters) and review and comparison of information on written documents and in the CTRS System by CRC staff as well as verifying the information with the Complainant when reviewing the EEO claim.

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

The following legal authorities are applicable for the CTRS OEE component of the CTRS System:
o Title VI of the Civil Rights Act of 1964
o Rehabilitation Act of 1973 Sections 504 & 508
o Age Discrimination Act of 1975
o Title IX, Education Amendments of 1972
o Job Training Partnership Act Section 167
o Section 188 of the Workforce Investment Act of 1998 Section 188
o Title II Subpart A of the Americans with Disabilities Act of 1990
o Executive Order 13160
o Secretary's Order 4-2000
o Section 188 of the Workforce Innovation and Opportunity Act
o Executive Order 13166
o Section 508 of the Rehabilitations Act of 1973
o Executive Order 11478
o Title VII of the Civil Rights Act of 1964
o Equal Pay Act of 1963
o Age Discrimination in Employment Act of 1967
o Rehabilitation Act of 1973 Sections 501, 504 & 508
o Pregnancy Discrimination Act
o Genetic Information Non-Discrimination Act
o Civil Service Reform Act of 1978
o Secretary's Order 2-81 & 3-96

- Privacy Impact Analysis

When personal information is gathered and stored there is a level of risk involved, such as identify theft or other fraudulent activities. Since the PII collected within CTRS System is initially captured via paper forms or emails, the information is safeguarded in secured file cabinets or in restricted areas where access to them is limited only to authorized personnel identification numbers and passwords. Electronic files and system access are controlled by means of identification numbers and passwords.

1.3 DESCRIBE THE USES OF THE PII

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

- Describe all the uses of the PII
  - Individual's name and contact information (business and home addresses, telephone numbers and email addresses) are used for identification and means of communicating status updates and other notifications.
  - Date of birth, race, color, religion, sex, disability, political affiliation, citizenship, reprisal/retaliation, national origin, genetic information, status as a parent and wages, are used to identify the EEO bases in claims of discrimination.
  - Medical information and device identifiers are primarily used for determining eligibility for disability reasonable accommodations.

- What types of tools are used to analyze data and what type of data may be produced?
  - CTRS System does not use any tools for data analysis; thereby, no other additional data is produced.

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
  - No, CTRS System does not derive new data or create previously unavailable data about an individual.
  -
- If the system uses commercial or publicly available data, please explain why and how it is used.
  - CTRS System does not use commercial or publicly available data.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?
  - No

- Privacy Impact Analysis
  - A complainant's complaint forms are stored in secured file cabinets, in restricted areas, where access is limited only to authorized personnel. Electronic files and system access are controlled by means of identification numbers and passwords.

1.4 RETENTION

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

- What is the retention period for the data in the system?

- In accordance with General Records Schedule 1.0 Items 25, 26, 27 current CTRS System Records Retention Schedules are:
  - For CTRS OEE component of the CTRS System - Records in this system are destroyed after one to four years. (N1 GRS 92 3 item 25c2).
  - For CTRS Title VII component of the CTRS System - Records are destroyed 4 years after resolution of case. (N1 GRS 80 9 item 1).

- Is a retention period established to minimize privacy risk?

Retention period is established based on the need to reference the case once it is closed for the purposes of handling future complaints of the same nature from the same complainant, handling similar complaints from different complainants or reporting purposes.

Yes and to document agency operations.

- Has the retention schedule been approved National Archives and Records Administration (NARA)?
  - Yes, CTRS System records retention schedule have been approved by the DOL Records Officer and filed with NARA. The records are covered by the **General Records Schedules (GRS) 1** for Items 25, 26, 27**, GRS 3.1,** item 012 (DAA-GRS-2013-0005-0008), item 051 (DAA-GRS-2013-0005-0003), item 050 (DAA-GRS-2013-0005-0002) Permanent Records and **GRS 3.2**, item 010 (DAA-GRS-2013-0006-0001).
- Per M-O7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; What efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?
  - CTRS System collects minimal PII data and that is being assessed annually for applicability and will be eliminated if not required by business functions.
- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?
  - Yes
- How is it determined that PII is no longer required?
  - Data requirements are established by NARA and FOIA requirements.
- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.
  - As the information is used to directly reach points of contact and access is limited to employees responsible for working with those individuals, no anonymization or masking is feasible.

- Privacy Impact Analysis

    - The length of time information is retained provides for an effective retention period, allowing enough time to use the information as needed to complete the mission and is destroyed in a manner that is most effective and in compliance with the NARA. Within the Records Schedule for EEO and OE records, CRC retains the temporary records on cases for four years following the complete closure of the case. After that four year period, the records are destroyed via approved DOL procedures. Permanent records are transferred to the National Archives with the permanent electronic records to which the documentation relates. Inappropriate use of the PII collected

1.5 INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

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

    - All PII captured within the OEE component of the CTRS System (see section 1 for information collected) is shared with Office of Federal Contract Compliance Program (OFCCP) when a complainant alleging discrimination pertaining to a federal contract. PII is also shared with the: Employment and Training Administration (ETA) when an applicant alleges discrimination related to an ETA program; Office of Workers' Compensation, when an applicant alleges issues pertaining to workplace injuries by Federal employees; Wage and Hour Division when the complaint alleges issues associated with unpaid wages; Employee Benefits Security Association when complaint alleges issues associated with health or retirement issues in private employment; Occupational Safety and Health Administration when the complaint alleges issues associated with workplace safety; and, Office of Inspector General when complaint alleges discrimination based on fraud in DOL programs or various types of inappropriate behavior by DOL employees.
    - All PII captured within Title VII component of the CTRS System (see section 1 for information collected) is shared with the Agency Workplace Equality Compliance Officers (WECOs) to assist WECOs with accessing information needed to car you their responsibilities as they pertain to monitoring and addressing EEO complaint matters in their respective DOL agencies.. The WECOs' agency responsibility includes, but is not limited to the following nine (9) large/major internal DOL agencies: Bureau of Labor Statistics (BLS) , Office of Workers' Compensation Programs (OWCP), Wage & Hour Division (WHD), Employment & Training Administration (ETA), Mine Safety & Health Administration (MSHA), Office of the Assistant Secretary for Administration & Management (OASAM), Office of Inspector General (OIG), Occupational Safety & Health Administration (OSHA), Employee Benefits Security Administration (EBSA) and Office of the Solicitor (SOL).
    - PII is shared with the SOL once case is sent to EEOC (when complainant elects to go in front of the EEOC Administrative Judge). DOL agencies not listed above are the responsibility of the OASAM WECO.

- How is the PII transmitted or disclosed?

    - PII within OEE component of the CTRS System is transmitted via DOL's internal mail or email. PII within Title VII component of the CTRS System is not transmitted as the WECOs have direct access to the system. The identified PII is transmitted internally between the CTRS regional/district/area offices and the national office through CTRS. This information is transmitted electronically and is only disclosed to those employees on a "need-to-know" basis.

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

    - Not applicable; the information is maintained in CTRS to support FOIA and NARA requirements, and potential future investigations.

- Privacy Impact Analysis

    - PII that is transmitted through DOL's interoffice mail system is marked confidential and sealed. Information transmitted through electronic review is protected through implementation of confidentiality and integrity controls. The impact of compromise to information through transmission is low.

1.6 EXTERNAL SHARING AND DISCLOSURE

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

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

    - In the event that a discrimination case file falls outside of DOL's jurisdiction for the OEE component of the CTRS System, the entire complainant's case file (paper form) is then forwarded via United Parcel Service (UPS) or United States Postal Service (USPS) to the appropriate federal agency that is responsible for processing and now resolving the complaint or it is sent electronically by email. Other federal agencies that may have impact are: Department of Labor (DOL), Department of Education (DOE), Equal Employment Opportunity Commission (EEOC), (federal and/or state level) Health and Human Services (HHS), and the Department of Transportation (DOT)This list could include any Federal or state agency depending on the substance of the complaint. Medical information within Title VII component of the CTRS System is shared with the Public Health Service (PHS). PHS assists in determining whether individuals are eligible for reasonable accommodations based on their disability.

- Is the sharing of PII 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 PII outside of DOL.

  - Yes, the sharing of PII outside of the Department is compatible with the original collection, and is addressed in SORN (DOL/OASAM-22) for OEE component of the CTRS System: https://www.dol.gov/sol/privacy/dol-oasam-22.htm As well as in SORN (DOL/OASAM-17) for Title VII component of the CTRS System: https://www.dol.gov/sol/privacy/dol-oasam-17.htm

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

  - Information is transported via United Parcel Service (UPS) or USPS carrier for the CTRS System or by email. The PII is in paper form and enclosed in a sealed envelope with a shipping label containing the recipient's name, mailing address, and delivery signature block.

- How is the information transmitted or disclosed?

  - Via paper documents and CDs in sealed envelopes shipped via UPS

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If yes, include who the agreement is with and the duration of the agreement.

  - No.
- How is the shared information secured by the recipient?

  - Documents sent to and from non-DOL emails are password protected. Documents uploaded to the shared site with USPS require two-factor sign on requirements.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

  - N/A

- Privacy Impact Analysis

  - There is privacy risks associated with personal information being handled by a third party. Should the United Parcel Service (UPS) or USPS envelope become lost, stolen or tampered with in any way the complaints information is vulnerable to identity y theft or other fraudulent activities. In order to mitigate this potential issue, information should be transmitted in electronic media only (e.g. disc, flash drive…etc.) with encryption to safeguard against unauthorized access to PII.

1.7 NOTICE

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

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.

    - Yes, notice is provided to individuals prior to collection of PII. The DOL website that hosts this application identifies the Privacy and Security statement for review by applicants. http://www.dol.gov/oasam/programs/crc/YourRightsEEO.htm

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

    - Yes, individuals have the opportunity and/or right to decline to provide information.

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

    - Yes, individuals have the right to consent to particular uses of the information. For instance, applicants do not have to reveal any personal information to CRC, but CRC may close users complaint if they refuse to reveal information needed to fully investigate complaint. The form also contains information on the "notice about investigatory uses of personal information" link. http://www.dol.gov/oasam/programs/crc/CIF-Notice.htm

- Privacy Impact Analysis

    - The privacy risk identified would be the failure of individual to know that his/her information may be collected and what it will be used for. The Civil Rights Center (CRC) provides a public website (http://www.dol.gov/oasam/programs/crc/complaint.htm) which explains the complaint process. Potential EEO complainants have prior access to the complaint form where they can view what would be expected of them or how the information will be used.

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

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

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

    - None – due to the sensitive nature of the information collected complainants are not allowed to directly access their information. However, they can request a status of their complaint and information will be provided via email or US mail. with the assigned compliance officer(s). The identified PII is entered into the CTRS, which is collected on the Informal Complaint Form and Formal Complaint Form.

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

    - If inaccurate or erroneous information was initially identified by CRC staff or other EEO designated staff/users, typically a phone call is placed advising of the situation and the corrective actions needed. An official correspondence on DOL Letterhead is sent to the individual notifying them of the corrected information.

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

    - An official correspondence on DOL Letterhead is sent to the individual notifying them of the corrected information.

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

    - This is not applicable as the Civil Rights Center's staff makes every effort to rectify inaccurate or erroneous information and inform individuals of issues and what corrective actions have been taken to address them.

- Privacy Impact Analysis

    - There is no additional risk in redress process as the public does not have direct access.

1.9 TECHNICAL ACCESS AND SECURITY

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

- Which user group(s) will have access to the system? (for example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

    - Access is limited to CTRS employees, and the contract staff responsible for supporting the system.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA.

    - Limited contractors in the support side have access to CTRS System. They also need to register and sign the Rules of Behavior.

- Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.
-

    - There are three levels of access for CTRS processing system
      Administrator: This level has the ability to work through all sections of the system which Include adding/deleting of records and all manipulations.

- Manager: This level has the ability to create new records, view all records, create/view reports but there are sections of the system that this level may not access and this level cannot delete records.
- User: This level only has the ability to view the records. The records for these users are in a locked format and cannot be altered by these persons. This level does have the ability to view automatically generated reports and produce ad-hoc reports.

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

  - Formal user access and account management procedures are in place to grant access to the system. Agency Approval of User Access and the CTRS System Rules of Behavior are two of the documented products within the guidelines established by OCIO and CRC.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided? Provide date of last training.

  - Roles are established and managed by CTRS managers. Managers cannot elevate a user above their own privileges. CTRS has implemented the Rules of Behavior which must be reviewed and signed by the individual as part of the account creation process. Employees participate in mandatory Privacy Act and Records Management training annually. This is provided by Learning Link, and so no single hard date is available.

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

  - Employees participate in mandatory Privacy Act and Records Management training annually. This is provided by Learning Link, and so no single hard date is available.

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

Physical records are maintained in a secured file room, file cabinets or in restricted areas, access to which is limited to authorized personnel. Electronic files are controlled by means of identification ID and passwords. CTRS supports:

- Authenticator/Password Management – Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management – Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review.
- Access Enforcement – Application and monitoring of access privileges.
- Least Privilege – Access to system's data is limited to data necessary for specific user to perform his/her specific function.
- Unsuccessful Login Attempts – System automatically locks

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

- The data is secured in accordance to FISMA requirements and the last Assessment and Authorization was completed on 2/23/2023

- Privacy Impact Analysis

  - The primary risks associated with the handling of privacy data include fraud and the unauthorized release of data outside of the controls of CTRS System. Office of Assistant Secretary for Administration and Management (OASAM) has implemented a required Security Awareness Training program, which includes the proper handling of privacy data. All staff members must complete online training. This year's training was entitled, the Information Systems Security and Privacy Awareness online training. All CTRS System users must also read and sign a Rules of Behavior document that outlines the expectations that CTRS System has for all staff members who handle privacy data. CTRS System has also implemented various auditing functions to track changes to the data. Also, online training has been implemented to ensure the proper handling of privacy data according to job function. CTRS System has also implemented various auditing functions to track changes to the data. The logical and physical access controls as identified in the CTRS System SSP mitigates the risks

1.10 TECHNOLOGY

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

- Was the system built from the ground up or purchased and installed?

  - The system was custom-designed and built.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.

  - The requirement to implement security and privacy controls were addressed in the system acquisition contract for CTRS.

- What design choices were made to enhance privacy?

  - CTRS employs technical controls and mechanisms, such as encryption, to enhance privacy.

- For systems in development, what stage of development is the system in, and what project development life cycle was used?

  - CTRS has been implemented and is currently being used at the production level.

- For systems in development, does the project employ technology which may raise privacy concerns? If so, please discuss their implementation?

- Not applicable. Security was built into the design of the system.

1.11 DETERMINATION

- As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

    - OCIO has completed the PIA for CTRS which is currently in operation. OCIO has determined that the safeguards and controls for this moderate system adequately protect the information.
    - OCIO has determined that it is collecting the minimum necessary information for the proper performance of a documented agency function.

1.12 PIA SIGNATURE PAGE

Responsible Officials

TRUDI NICHOLS Digitally signed by TRUDI NICHOLS Date: 2023.04.10 10:02:33 -05'00'

_____

Signature of System Owner

04/10/2023

_____

Date

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; email address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for ■ Federal employees, ☐ Contractor staff, ☒ Members of the Public {Check all that apply}

- ■ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ■ First name ■ Middle initial and/or ■ Last name
- ■ Name suffix such as Jr. Sr., etc.
- ■ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ■ Language spoken
- ■ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ■ Residential address
- ■ Personal phone numbers (e.g., phone, fax, cell)
- ■ Mailing address (e.g., P.O. Box)
- ■ Personal email address

- [x] Business address
- [x] Business phone number (e.g., phone, fax, cell)
- [x] Business email address
- [x] Medical information including physician's notes
- [x] Medical record number
- [ ] Device identifiers (e.g., pacemaker, hearing aid)
- [ ] Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- [ ] Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- [ ] Certificates (e.g., birth, death, marriage)
- [ ] Legal documents or notes (e.g., divorce decree, criminal records)
- [ ] Educational records
- [ ] Network logon credentials (e.g., username and password, public key certificate)
- [ ] Digital signing or encryption certificate
- [ ] Other: _____
- [ ] None

- Is any part of the PII collection voluntary?

  CTRS PII collection is voluntary.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

  As the information is used to directly reach points of contact and access is limited to employees responsible for working with those individuals, no anonymization or masking is feasible.