PRIVACY IMPACT ASSESSMENT (PIA)

For the

CONTRACT LINGUIST ENTERPRISE DATABASE (CLED) NIPR
US ARMY G-2

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- [x] **New DoD Information System**
- [ ] **New Electronic Collection**
- [ ] **Existing DoD Information System**
- [ ] **Existing Electronic Collection**
- [ ] **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- [x] **Yes, DITPR** Enter DITPR System Identification Number: 13121 (DA201156)
- [ ] **Yes, SIPRNET** Enter SIPRNET Identification Number:
- [ ] **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- [ ] **Yes**
- [x] **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- [x] **Yes**
- [ ] **No**

If "Yes," enter Privacy Act SORN Identifier A0025-2d CLED NIPRNet

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office 5 March 2010
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Per the Privacy Act SORN DMDC 12 DoD, the authorities to collect information are:
5 U.S.C. 301, Departmental Regulations
Executive Order 12356,
Executive Order 10450,
Executive Order 9397,
DoDD 8500.1, Information Assurance,
AR 25-2, Information Assurance,
E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Contract Linguist Enterprise Database (CLED)- Non-Classified Internet Protocol Network (NIPRNet) is a single enterprise database with interfacing architecture to allow accountability and management of all contract linguists including all local nationals, their languages/dialects, current location, work history, and security clearance status. CLED resides on NIPRNet that will assist the Army, and imports all existing data and operational functions conducted by Contractor Translator Interpreter Data Entry System (C-Tides) (Army Intelligence and Security Command (INSCOM)-CLPSO) contract linguist personnel information database), Theater Linguist Manager, Vendor specific databases and Army Knowledge Online (Army Contract Linguists Eligibility Files).

Phase -1 The enterprise database interfaces with Contract Linguist Information Portal (CLIP) (Army G2X (CI/Humint Advisor)-Language Support Office (LSO) linguist CI/FP vetting database), Army Contractor Automated Verification System (ACAVS) (INSCOM-Contractor Support Element (CSE) Sensitive Compartmented Information (SCI) eligibility and contract verification database) PSIP(Personnel Security Investigation Portal) and CATS (Clearance Adjudication Tracking System - Army Central Clearance Facility).

Phase -2 During this phase the database interfaces with PSIP (Army CCF), JPAS (DoD Defense Security Service (DSS),Industrial Securities Facilities Database (ISFD) (DoD DSS), ACAVS, CVS (Contractor Verification System), Synchronized Pre-deployment and Operational Tracker (SPOT) (Army Material Command (AMC), DCII (Defense Clearance Investigation Index -DSS), Scatter Castlefeed Director of National Intelligence (DNI) and BIR (Biometrics Information Repository - National Ground Intelligence Center (NGIC). Data will be shared with other Federal Agencies such as Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA) and others. Contractors such as Mission Essential Personnel(MEP) and Global Linguist Solutions (GLS) will enter data into the database.

This application has been directed to be developed to support the oversight of contractor linguists availability and performance in support of the United States Government. This single enterprise database repository will interface with other DoD and Agency repositories to ensure accountability and management of all US hired contract linguists, local national contract linguists, their language(s)/dialect(s), current location, security clearance category, work history and security clearance status. Once operational the database will allow authorized DoD entities to input, request, and track their contract linguists. The information contained will not be released to the public.

PII collected include personal, employment, financial, and educational.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collected are the unauthorized release of PII data. These risks are addressed by protecting the data collection resource with strong Secure Sockets Layer (SSL) encryption, programmatically restricting the system from releasing PII data through its interfaces, through SSL encryption with Common Access Card (CAC) of PII released to partner agencies under the routine use guidelines authorized in the Privacy Act System Of Record Notice (SORN), through periodic Information Assurance training of personnel with access to the PII, and through access control restricted by CAC to internal network personnel whose job functions require access to PII. Moreover, those authorized security personnel with access to the CLED have a favorably adjudicated Single Scope Background Investigation.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. ARMY G-2, Army Intelligence and Security Command, National Ground Intelligence Center, and all other agencies with a need to know in order to perform their duties.

☒ **Other DoD Components.**

Specify. Defense Security Service and all Department of Defense agencies with a need to know in order to perform their duties.

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigation, Central Intelligence Agency, and all Federal agencies with a need to know in order to perform their duties.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Mission Essential Personnel, Global Linguist Solutions and other vendors, see FAR 39.107 and 52.239.1 incorporated by reference. Appropriate safeguards are in place during collection, use, retention, processing, disclosure and destruction. Information is protected by user passwords, firewalls, anti-virus software, Common Access Card access and data-at-rest protection software on laptops. Access to the data is at least privilege. All data is encrypted in a database, appropriate safeguards are in place for the collection, use and sharing of information, security measures are adequate and risk is minimal. Appropriate safeguards are in place for the collection, use and sharing of information. Information is protected by user passwords, firewalls, antivirus software, Common Access Card access and data-at-rest protection. PII are encrypted and saved in database and individual account numbers are generated.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

At the time individuals initiate the personnel security process they are requested by their employing agency's security office to execute the Office of Management and Budget approved, Office of Personnel Management administered, Standard Form 85, Standard Form 85P, or Standard Form 86 as determined by the purpose of their investigation. These forms inform individuals that providing the requested personal information is voluntary and the disclosure of information and routine uses are explained. When an individual completes any of these forms and signs the applicable authorizations for release of information the individual is consenting to the collection of PII. Conversely, the individual can object to the collection of PII by not completing these forms and signing the applicable authorizations of release, at which time the process ceases.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The individual is able to object, as cited in 2.i.(1); however, once the information is collected the individual is unable to pick and choose how the information will be used during the conduct of the adjudication for access to information.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☒ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.

Personal data is voluntarily given by the applicant and collected via electronic or manual forms. Forms requesting privacy information contain an applicable privacy statement. Privacy Act Advisory Statements are displayed upon log-in to the system.

All applicant records in CLED, have the following regulatory notices as part of the personnel record: Social Security Number: A social security number is requested under the authority of Executive Order 9397 to uniquely identify records of applicants who may have the same name. Also, as allowed by law or presidential directive, a social security number is used to map candidates' records to their corresponding personnel files and assign a unique CLED record.

Privacy Act - Privacy Act notice: The information requested here is used to manage candidate information and adjudicative decisions.