PRIVACY IMPACT ASSESSMENT (PIA)

For the

Retroactive Stop-Loss

US Army Deputy Chief of Staff for Personnel / Human Resources Command (HRC)

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:

- ☐ **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?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 12186 (DA195584)
- ☐ **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**
- ☒ **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.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier: A0690-200 DAPE

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
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.

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 3013, Secretary of the Army
Army Regulation 690-200, General Personnel Provisions
Executive Order 9397, Authorization to use SSN as a personal identifier, 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.

Retroactive stop-loss system will be used to collect current information for distribution of payments for members (including reserve and retired personnel) who served for an extended period between September 10, 2001, and September 30, 2008, under the President's stop-loss authority as part of the 2009 war supplemental funding bill HR2346, Public Law 111-32 section 310. The claims can be filed over the next year. If a claimant misses the one-year window the claim will not be paid.

The purpose of collecting this information is 1) verification of the person 2) collect current contact information including beneficiary's and direct deposit information for payment to that individual who served for an extended period between September 10, 2001, and September 30, 2008, under the President's stop-loss authority are part of the 2009 war supplemental funding bill HR2346.

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

Privacy risks for collecting this data include the home address, bank account and possibly the beneficiary of an individual. These risks are addressed by restricted areas accessible only to authorized personnel with documented security clearances. Physical access is controlled by dual access controls, alarm system, surveillance system, properly cleared and trained personnel with approved need-to-know, and computer hardware and software security features. Records are restricted to designated personnel and protected by a layered architecture and data encryption. Protection is commensurate with the sensitivity level of the data.

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. All Army components and major commands which includes Active, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Inspectors General, Army Intelligence and Security Command, Army Reserves, Assistant Secretary of the Army (Financial Management & Comptroller) , Department of the Army Inspectors General, Provost Marshal General, Army Staff Principals in the chain of command, and Supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

☒ **Other DoD Components.**

Specify. Routine;
Defense Finance and Accounting Service,

As Requested;
Defense Criminal Investigative Service, Defense Integrated Military Human Resources System, Defense Manpower Data Center, Defense Security Service, Department of Veterans Affairs, DoD Inspector General, National Guard Bureau, Office of the DoD Inspector General, Office of the Secretary of

Defense, Office of the Secretary of Defense Personnel and Readiness.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

An individual has the opportunity to decline consent to the DoD warning banner which not allow them into the system to enter their information into to collect the claim.

(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 does not control the specific uses of the PII data once collected into the RSL system. The data is only used to verify the individual's identity and confirm their stop-loss status with current contact 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.

You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.

Privacy Act Statement AUTHORITY: Public Law 111-32, Section 310; E.O. 9397.

PRINCIPAL PURPOSE(S): Solicitation of information contained herein may be used as a basis for retroactive stop loss pay determinations. Your information will be used by the Services, for verification of eligibility and then by the Defense Finance and Accounting Service for payment of Retroactive Stop Loss payments. The Military Departments describe how your information will be maintained in their Privacy Act System of Record Notice.

ROUTINE USE(S): The DoD "Blanket Routine Uses" apply.

DISCLOSURE: Voluntary; however, failure to provide information requested on this form may result in the government's inability to provide benefits under the stop loss pay program. Your Social Security Number is being requested pursuant to E.O. 9397. The SSN and other identifying information are needed to pay the proper person, ensure entitlement to benefits, and for tax purposes.

User Agreement By using this IS (which includes any device attached to this IS), you consent to the following conditions: •The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
•At any time, the USG may inspect and/or seize data stored on this IS.
•Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
•This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
•Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.