PRIVACY IMPACT ASSESSMENT (PIA)

For the

Deputy Chief of Staff G-2 NIPRNET LAN
Office of the Deputy Chief of Staff, Military Intelligence

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: 12944 (DA 199348)
- ☐ **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

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.

Collected for internal housekeeping by supervisors for recall rosters; by personnel office to verify employment eligibility; by security manager for clearance actions; by budget office for travel expenses. Various authorities include: Sections 1302, 5532, 6311 Title 5 US Code; Title 8 USC; 31 USC 3322, 31 CFR 209 and/or 210; Executive Orders 11190, 9397, and 10450; and Public Law 99-474, the Computer Fraud and Abuse Act.

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.

The G-2 unclassified Local Area Network (LAN) allows personnel to connect to other DoD and Federal agencies and offices and to the Internet. Users must logon with their Common Access Card before they can access any items or web sites. PII stored on network servers is used to confirm employment eligibility, to verify security clearance, for supervisors' contact lists, for payroll and travel.

The Deputy Chief of Staff, G-2 unclassified LAN is an Organizational Unit (OU) of the Military Intelligence (MI) Forest providing an office automated information network comprised of 28 servers, 550 workstations, printers, visual information suites, plotters, video teleconferencing suites, digital senders, Domain Name Service, NETAPPS Filers, and web services. This LAN is connected to the MI Forest via tunneling through the HQ Department of the Army (DA) Pentagon backbone. This LAN supports the DCS, G-2 personnel, the Antiterrorism Operations and Intelligence Cell, and other external HQDA staff as approved by the Designated Approving Authority. This OU supports the following sites, Carlisle Barracks (PA), Site R (PA), Skyline (Contractor-Owned Government-Operated) site (Alexandria,VA), the Pentagon (Washington DC), and Presidential Towers (Crystal City, VA).

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

Internal and external risks are associated with the protection of PII; however, risks are minimized to an acceptable level. Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus the risk to the individual's privacy to be minimal.

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. Some Army components and major commands which includes Active, Army Accessions Command, Army Audit Agency, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Inspectors General, Army Intelligence and Security Command, Assistant Secretary of the Army (Financial Management & Comptroller), 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. Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Security Service.

☐ **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.

PII is required for payroll, clearance actions, contact lists, access to government computer systems and information, and employment. The individual tells the office requesting the information that they do not wish to give it. However, failure to provide the requested information may impede, delay or prevent further processing of the leave request, employment application, system access request.

(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.

Since the information is used for payroll, employment, access to DoD computer systems and information, and clearance actions, which are required to hold the job, and for office contact lists, refusal to allow use of their PII for these actions may result in a loss of job.

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

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

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

PII words from the Privacy Act Statement on Civilian Leave Form:
Section 6311 of Title 5, United States Code, authorizes collection of this information. The primary use of this information is by management and your payroll office to approve and record your use of leave. Additional disclosures of the information may be: to the Department of Labor when processing a claim for compensation regarding a job connected injury or illness; to a State unemployment compensation office regarding a claim; to Federal Life Insurance or Health Benefits carriers regarding a claim; to a Federal, State, or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to a Federal agency when conducting an investigation for employment or security reasons; to the Office of Personnel Management or the General Accounting Office when the information is required for evaluation of leave administration; or the General Services Administration in connection with its responsibilities for records management. Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish a social security number or tax identification number. This is an amendment to Title 31, Section 7701. Furnishing the social security number, as well as other data, is voluntary, but failure to do so may delay or prevent action on the application. If your agency uses the information furnished on this form for purposes other than those indicated above, it may provide you with an additional statement reflecting those purposes.

PII words from Systems Authorization Access Request form:
Authority: EO 10450, 9397, and Public Law 99-474, the Computer Fraud and Abuse Act.
Principal Purpose: to record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to DoD systems and information.
Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.