PRIVACY IMPACT ASSESSMENT (PIA)

For the

DCS G-2 SIPRNET - HQDA DCS G-2 SIPRNET LAN

Office of the Deputy Chief of Staff, 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:

- ☐ **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: 13775 DA200732
- ☐ **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.

This is NOT a system of records, is not a collection source and does not collect from the general public.

The presence of PII is through routine uses and internal housekeeping to conduct Army business, the information is for controlled internal cybersecurity processes executed by appointed automation points of contact (APOC)for system access requests coordinated through the Information Systems Security Manager or Officer (ISSM or ISSO), Help Desk and Security Manager; by an appointed Inquiry Official investigating a potential security violation; 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 HQDA DCS, G-2 SIPRNet LAN is an OU of the Collateral MI Forest providing an office automated information network comprised of 18 servers, 499 workstations, (additional resources include printers, visual information suites, plotters, video teleconferencing suites, digital senders, DNS, and network attached storage), with primary web and file services operating using MS Win 7 OS and on MS 2008R2 and 2012R2 servers. This LAN is connected to the MI Forest via tunneling through the HQDA Pentagon backbone. This LAN supports the HQDA ODCS, G-2 personnel, the ATOIC, and other external HQDA staff as approved by the AO. This OU supports the following sites: the Pentagon (Washington DC), Taylor Buildings (Crystal City VA) and remote COOP sites.

This system is not a source of collection, personally identifiable information is NOT collected on the public and information in DCS G-2 SIPRNet is not released to the public, nor any public entity. The system has been used to temporarily maintain specific documents containing details relating to in-processing of personnel, coordinated through their Automation point of Contact (APOC), Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), Help Desk and Security Manager for system access approval request processing and approval. An appointed Inquiry Official investigating an individual for potential security violation may also obtain a dossier about an individual from the DoD Consolidated Adjudications Facility (DoD CAF) during the investigative process of security incident review. The level of personally identifiable information (PII) is limited to the details necessary to determine which individual requires system access and to confirm their need-to-know approval from their director.

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

As part of a national security system, the risk to privacy of collected PII is minimized by the protections afforded all data on this classified system, but further protected by restricting access to such information to those specifically authorized access; SA, Security Managers and ISSM/ISSO when applicable. This includes enabled encryption capabilities and partitioned file shares limiting accesses to directorates and specified groups. Retention of PII, IAW Army Regulation 25-22, Army Privacy Program, is limited to the duration of a given requirement and must be removed once completed. All storage media that reaches end-of-life, must be controlled and destroyed as classified waste.

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. The PII is shared between a directorate's Director, APOC, the ISSM/ISSO, a Security Manager and Help Desk personnel. Documents containing PII as a result of an investigation will be exchanged between an Inquiry Official, the DoD CAF and director, when applicable. Additional coordinations are occasionally necessary between the Help Desk personnel and INSCOM.

☐ **Other DoD Components.**

Specify.

☐ **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.

All DD Form 2875, System Access Authorization Request (SAAR) forms and DCS G-2 Access Request forms have a Privacy Act Statement included to indicate each individuals option to object to PII collection. The version of the DD Form 2875 used within G-2 no longer requests, nor uses any SSN or truncated variation. Due to the controlled process of obtaining a dossier from the DoD CAF for incident investigations, the Privacy Act Statement restricts the authorized use of the PII to the investigative proceedings between the DoD CAF and the Inquiry Official.

(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.

As with all the forms used for PII, in whole or in part, the Privacy Act Statement allows for the full disclosure of information and details the intended use is strictly for the purposes of evidence collection or system access approval. The individual can refuse, in whole or in part, with the understanding that failing to provide the requested details may prevent system access approval or limit the ability to properly distinguish their involvement in an incident at an investigative level. This limit could result in temporary suspension or complete termination of an individuals clearance authorization.

(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.

☒ **Privacy Act Statement**	☐ **Privacy Advisory**
☐ **Other**	☐ **None**

Describe each applicable format.

The following forms and their Privacy Act Statements apply:

DD FORM 2875:
Authority - Executive Order 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 Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
Routine Uses - None.
Disclosure - Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

DCS G-2 Access Request:
NOTE: The Privacy Act, U.S.C. 552a., requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your SSN, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

DoD CAF Individual Dossier

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.