



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

G-3/5/7 Personnel Database (G3PDB)

Army

### 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
- 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.

SORN is under review

**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.

DoD 5400.11-R, "Department of Defense Privacy Program", May 14, 2007

DTM-2007-015-USD (P&R), para (3, 4,5),(8,9) and (12)

Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Employees and Contractors," August 27, 2004

DoD Directive 5101.1, "DoD Executive Agent", September 3, 2002

Section 112 of the Emergency Supplemental act of 2000, Pub. L. No. 106-246, July 13, 2000

**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-3/5/7 Administration and Resources Directorate provides Human Resources support to over 2,100 personnel in support of the Army G-3/5/7 mission. The G3PDB provides operational support for day-to-day personnel activities. The PII collected support the following: Military personnel identification, DA and DD forms for movement orders and finance, awards, evaluations, Government Travel Card and DTS transactions, Security clearance requests, Pentagon Badges, civilian personnel actions and evaluations/finance transactions, class registration for training courses, emergency alert notification systems. The database also has AD HOC capabilities for short notice requests for information from the G-3 leadership and can produce recurring reports. The type of PII collected is personal, military, employment, work-related, and educational information.

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

The risks associated with the PII data collected by the G3PDB include loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

All DoD employees and contractors are required to take mandatory security and privacy training prior to accessing a DoD system. This security and privacy training course includes an overview of privacy, PII, and its appropriate uses. Additionally, the U.S. Army requires that all employees (DA Civilians, military and contractors) complete annual refresher IA and PII training. Further, all actions on the system are logged and maintained to ensure accountability.

Access Control: ZCA will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training: ZCA will: 1) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and 2) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability: ZCA will: 1) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and 2) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments: ZCA will: 1) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; 2) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; 3) authorize the operation of organizational information systems and any associated information system connections; and 4) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management: ZCA will: 1) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and 2) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning: ZCA will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication: ZCA will identify information system users, processes acting on behalf of users, or devices and authenticate or verify the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response: ZCA will: 1) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and 2) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: ZCA will: 1) perform periodic and timely maintenance on organizational information systems; and 2) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection: ZCA will: 1) protect information system media, both paper and digital; 2) limit access to information on information system media to authorized users; and 3) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection: ZCA will: 1) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; 2) protect the physical plant and support infrastructure for information systems; 3) provide supporting utilities for information systems; 4) protect information systems against environmental hazards; and 5) provide appropriate environmental controls in facilities containing information systems.

Planning: ZCA will develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for in the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security: ZCA will: 1) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; 2) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and 3) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment: ZCA will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition: ZCA will: 1) allocate sufficient resources to adequately protect organizational information systems; 2) employ system development life cycle processes that incorporate information security considerations; 3) employ software usage and installation restrictions; and 4) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection: ZCA will: 1) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and 2) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity: ZCA will: 1) identify, report, and correct information and information system flaws in a timely manner; 2) provide protection from malicious code at appropriate locations within organizational information systems; and 3) monitor information system security alerts and advisories and take appropriate actions in response.

**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.

HQDA G-3/5/7

**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 individuals requesting employment with ZCA must provide the requisite information in order to gain entrance to G-3/5/7 facilities and/or the G3PDB. An individual may refuse consent to specific uses of PII, however, the PII is required for the human resources and security operations staffs to perform their respective duties for the G-3/5/7. Refusal to provide the information will preclude the individual from obtaining a position with ZCA or access to the G3PDB.

(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.

Personal data is voluntarily given by applicants and collected via other electronic means. A privacy Act