PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Freedom of Information and Privacy Acts Case Tracking System (FACTS)

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

08/25/20

Office of the Administrative Assistant (OAA) to Secretary of the Army
U.S. Army Records Management & Declassification Agency

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

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

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

The Freedom of Information and Privacy Acts Case Tracking System (FACTS) will not be found in eMASS as it is listed as a child application under ARIMS in APMS. FACTS is a web-based enterprise solution, which provides uniformity of data collected during administratively processing of FOIA/PA cases, facilitates world-wide tracking and exposure, empowers users to search case information on an Army-wide or activity-specific scale, and employs automated programs and management reports. Access to FACTS is limited to Army FOIA/PA Officers, IDAs, and other individuals authorized to process and respond to requests from individuals and corporations outside the Federal Government. Users are authenticated by Army Knowledge Online (AKO) and CAC Login for access to the system.

User's PII collected consist of names, addresses, to include email, phone number. Member's of the public personal information, such as mailing address and phone number is keyed into the system upon receipt of a written request for records.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Information is solicited for the purpose of verifying the user's identity during the login process; and to correspond with the FOIA requester.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Disclosure of the user's information is voluntarily. Information is solicited for the purpose of verifying the user's identity and corresponding with the requester. Failure to provide the requested information will result in denial of access to FACTS and failure to receive requester records.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

Information is solicited for the purpose of verifying the user's identity and corresponding with the requester. Failure to provide the requested information will result in denial of access to FACTS and failure to receive requester records.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

- [ ] Privacy Act Statement
- [ ] Privacy Advisory
- [x] Not Applicable

h. **With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

[X] Within the DoD Component	Specify.	All Army components and major commands which includes Active, Army Accessions Command, Army Audit Agency, Army Cadet Command, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Inspectors General, Army Intelligence and Security Command, Army Recruiting Command, Army Recruiting Information Support System, Army Research Institute, Army Reserve Command and to Commanders, Army Reserves, Army Training and Doctrine Command, 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.
[X] Other DoD Components	Specify.	PII information encoded on users CAC
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Hexagon US Federal (Formerly Intergraph Government Solutions). Personal Data and Personally Identifiable Information (PII) Compliance with Privacy Act - Contractor must comply with the Personally Identifiable Information requirements as set forth in the Privacy Act of 1974, Public Law 93-579, as amended, including all policies and directives issued therein including, for example, DoD Directive 5400-11, DoD Program dated May 8, 2007, as may also be amended from time to time or superseded.
[ ] Other *(e.g., commercial providers, colleges).*	Specify.	

i. **Source of the PII collected is**: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

j. **How will the information be collected?** *(Check all that apply and list all Official Form Numbers if applicable)*

- [X] E-mail
- [X] Face-to-Face Contact
- [X] Fax
- [X] Information Sharing - System to System
- [X] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [X] Paper
- [X] Telephone Interview
- [X] Website/E-Form

The information is manually entered by an authorized FACTS user. PDF records may also be scanned and entered into the system.

k. **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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier A0025-55 OAA

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date 11 July 2014

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 4.2, item 30 (DAA-(

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

KE2. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

5 U.S.C. 552, Freedom of Information Act, as amended by Pub.L. 93-502; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 25-55, The Department of the Army Freedom of Information Act Program; and E.O. 12958, National Classified Security Information, as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.