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:

Electromagnetic Battle Management Joint Decision Support (EMBM-J DS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

04/12/24

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees
- [ ] from both members of the general public and Federal employees
- [ ] 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.

EMBM-J DS provides planning and management capabilities, enhanced Electromagnetic Spectrum (EMS) Decision Support (DS), and improved interoperability with related service, joint and intelligence tools, and systems. EMBM-J DS is a browser-based application delivered to user's desktop and does not require the installation of software on a user's workstation. The type of PII that is collected includes: Name(s), DoD ID Number, Work Email Address.

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)*

Identification and verification of an individual requesting access to use services.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] 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.

Individuals can object to the collection of PII by not completing and submitting the access request form.

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

Individuals can object to the specific uses of their PII by not completing and submitting the information required.

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.)*

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

Authorities: 5 U.S.C. 301. Departmental Regulation: DoD Directive 1000.25. DoD Personnel Identity Protection (PIP) Program:
Principal Purposes: To collect names, DoD ID number, work email address for the purpose or validating the trustworthiness or individuals requesting access to the Department or Defense (DoD) EMBM-J DS system.
Routine Uses: DoD 'Blanket Routine Uses' set forth at the beginning or OSD's compilation of systems of records notices apply to this system. See the applicable system or records notice for a complete listing of routine uses: K890. 14 DoD. ldSS located at

Disclosure: Voluntary. However, failure to provide or update your information may result in termination or refusal or access.

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

x	Within the DoD Component	Specify.	DISA
	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
	State and Local Agencies	Specify.	
	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.	
	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		Databases
	Existing DoD Information Systems		Commercial Systems
	Other Federal Information Systems		

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

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

Read from Common Access Card (CAC).

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 K890.14

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

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 3.1, GRS 3.2

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

(3) Retention Instructions.

3.1 General Technology Management Records
-001: Destroy when 5 years old, but longer retention is authorized if needed for business use.
-011: Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
-020: Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.
-030: Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

3.2: Information Systems Security Records
-010: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
-020: Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
-030: Destroy when business use ceases.
-040: Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.
-060: Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.
-062: Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule, or in the case of permanent records when the record is transferred to NARA legal custody. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period.

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.

The following authority allows Electromagnet Battle Management Joint Decision Support (EMBM-J DS) to collect the following data:
- USCYBERCOM TASKORD 15-0 I 02 Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication, July 15, 2015
- Secure Administration Authentication Gateway and Enterprise Privileged User Authentication Service, March 31, 2019
- DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, February 21, 2019
- DoD Instruction 8520.03. identity Authentication for Information Systems. February 21, 2019

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.

x 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.

OMB Control Number: 0704-0415
Expiration Date: None