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:

Global Electromagnetic Spectrum Information (GEMSIS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

03/19/2021

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
- ☐ 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
- ☒ 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.

Global Electromagnetic Spectrum Information System (GEMSIS) is the joint program of record that is transforming spectrum operations from a pre-planned and static frequency assignment into a dynamic, responsive, and agile capability.

GEMSIS provides an enterprise suite of spectrum management services integrated in a common data environment to improve operational access to spectrum resources. The web service enterprise environment allows for machine to machine information exchange.

The GEMSIS PMO mission is to develop, deploy, and sustain a joint information system of integrated spectrum capabilities that will enhance the Warfighter's ability to effectively and efficiently manage the electromagnetic battlespace to enable information superiority.

The GEMSIS PMO needs to collect this information to aide the authentication and authorization process for the user to access GEMSIS. Finally Email is collected in order to aid communication with the user.

PII is collected via CAC(EDIPI - DoD ID Number), name and work email address fields.

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)*

PII is collected via CAC(EDIPI - DoD ID Number) and work email address fields. This is required for the verification of users identification as well as being part of the GEMSIS authentication process.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ 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.

Users are required to have a CAC Certificate to gain access to all applications (ISD, JSDR and E2ESS) within GEMSIS. Individuals/users can object to the collection of their PII in the system if they chose not to utilize the GEMSIS service. However, individuals are unable to object to the collection of PII if using the service, in order to satisfy aforementioned GEMSIS service requirement.

f. 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.

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

Individual can consent to the specific uses of their PII in choosing whether or not to utilize the GEMSIS service. However, in order to establish a GEMSIS account, consent is mandatory.

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 ☐ Not Applicable

The information you provide to the Global Electromagnetic Information System (GEMSIS) program is covered by the Privacy Act of 1974. For questions regarding your personal information please contact the Defense Spectrum Organization Security Branch.

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 of validating the trustworthiness of individuals requesting access to the Department of Defense (DoD) GEMSIS system.
Routine Uses: DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system. See the applicable system of records notice for a complete listing of routine uses: K890.14 DoD, IdSS located at https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570712/k89014-dod/.
Disclosure: Voluntary. However, failure to provide or update your information may result in termination or refusal of access.

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

☒ Within the DoD Component	Specify.	DISA
☐ Other DoD Components	Specify.	
☐ Other Federal Agencies	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)*

☒ 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)*
☐ Face-to-Face Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☒ Information Sharing - System to System ☐ Website/E-Form
☒ Other *(If Other, enter the information in the box below)*

EDIP is pulled from CAC, Name and work email is pulled from Form 2875

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier K890.14 DoD

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 and 3.2. Various

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

(3) Retention Instructions.

001 Technology management administrative records. 020 Information technology operations and maintenance records. 030 Configuration and change management records. 010 Systems and data security records. 020 Computer security incident handling, reporting and follow-up records. 011 System Development Records. 030 System access records. 040 System backups and tape library records. 060 PKI administrative records. 062 PKI transaction-specific records.

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 authority allows Global Electromagnetic Spectrum Information (GEMSIS) to collect the data: 5 U.S.C. 301, Departmental Regulation; 10 U.S.C. chapter 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan for Persons and Personas; and Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS).

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.

OMB Control Number: 0704-0415; Expiration Date: None