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:

Spectrum XXI Version 5 (SXXI v5)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

09/01/23

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   □ 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

☒ 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.

SXXI is a mission essential National Security System (NSS) used by the Department of Defense (DOD) for strategic and tactical operations. The system is designated as the DOD's Joint Frequency Assignment system, and it has been in use operationally at the DOD since 1999. The system provides a suite of tools and workflow automation to process frequency requests and manage use of the electromagnetic spectrum (i.e., radio frequencies). DOD instances/versions of the system. SXXI follows a client-server architecture, and the SXXI client contains the following modules: Frequency Assignment, Interference Analysis, Electronic Warfare, Joint Restricted Frequency List (JRFL), Engineering Tools, Compliance, Allotment Plan Generator, Data Exchange, Topo Manager, Spectrum Certification System and System Tools. It inter-operates with the NTIA Federal Spectrum Management System and any system that complies with the Standard Frequency Action Format (SFAF) frequency record data standard. No existing Commercial-off-the-Shelf (COTS) system or other Government-off-the-Shelf (GOTS) system meets SXXI system requirements. SXXI operates in a closed loop architecture. SXXI desktop, laptop, or thin clients data exchange information to the servers. SXXI has no external APIs or other send/receive P2P send/receive connections. The sole exception is a one way data feed from SXXI to the Joint Spectrum data Repository. This ETL is one way, SXXI to JSDR and read only to the authorized user community. The types of PII collected are as follows: DoD ID Number and Work E-mail 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)*

DoD ID Number is collected in Oracle Wallet for users authenticating to the server via token to perform data exchange.

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.

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

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.

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.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

AUTHORITY: Executive Orders 10450, Security requirements for Government employment; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE(S): To collect 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 USE(S): None
DISCLOSURE: Voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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)*

☒ Within the DoD Component	Specify. DISA HaCC Stratus
☐ 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)*

☒ Individuals
☐ Existing DoD Information Systems
☐ Other Federal Information Systems
☐ Databases
☐ Commercial Systems

MIL, CIV & CTR personnel with approved access to the application.

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

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

SXXIv5 user's DoD ID number is stored in Database. DD 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

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

(3) Retention Instructions.

GRS 3.1:

001 Technology management administrative records: Temporary. Destroy when 5 years old, but longer retention is authorized if needed for business use.

011 System development records: 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 Information technology operations and maintenance records: Temporary. 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 Configuration and change management records: Temporary. 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.

GRS 3.2:

020 Computer security incident handling, reporting and follow-up records: Temporary. Destroy 3 years after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

030 System access records: Temporary. Destroy when business use ceases.

040 System backup and tape library records: Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

060 PKI administrative records: Temporary. 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 PKI transaction-specific records: Temporary. 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.

5 U.S.C 301, Departmental Regulation; 10 U.S.C Chapter 8; DoD Directive 5105.19, Defense Information Systems agency (DISA); DoD Directive 1000.25, Personnel Identity Protection (PIP) Program; DoD Enterprise User data Management Plan for Persons and Personas; 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