# 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:**

Joint Interoperability Test Command - Fort Huachuca

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

10/15/2021

## 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.**

JITC-FHU has a need to provide test and evaluation of the interoperability of DoD business and healthcare systems. The types of information collected and analyzed vary by test event and systems under test, but does frequently include information that falls under Personally Identifiable Information/Personal Health Information (PII/PHI) protection standards. The test customer sends the test PII/PHI data to JITC via encrypted data files that pass through the Network Integration Testbed (NIT) and Joint Data Management Tool (JDMT) web portal on their way to the System Integration Lab (SIL) server that houses the Joint Analysis Net Centric Evaluation Testing Toolkit (JANETT). This server stores the files for use by the testers. The testers then transfer this data to JANETT workstations and/or stand-alone laptops belonging to the EBS-STEL enclave for testing using the JANETT software tool. Once the test is complete, the PII/PHI data is deleted from the server as well the workstations/laptops and the workstations/laptops are re-initialized with a new Operating System (OS) load as well as other required software. No PII/PHI data used for purposes of this testing is originated at JITC nor is it disseminated outside of JITC.

JITC-FHU also has a need to provide real-world financial analysis and reporting regarding JITC federal employee labor charges in order to understand current and per-pay period charges as relates to project funding. JITC's primary need in this regard is to use the JITC Test and Evaluation (T&E) Dashboard for data collection and reporting of this information, as no other local system is available for this purpose.

The T&E Dashboard is a general-purpose web application that provides functions to track and report on information as requested by various JITC divisions and branches. The original intent for the application was to standardize and validate data entry for test areas such as Interoperability (IOP) and Standards Conformance Testing (SCT). Over time, the application has evolved to include individual needs from various JITC branches as well as receiving and reporting on information from the Defense Agencies Initiative (DAI) system. A select few individuals provide this information via data upload from DAI to the Dashboard. The information may, or may not, be permanently stored on the Dashboard server. These files are not passed to any other systems. The information from these uploads are stored in the Dashboard's database and used for reports on the application.

The system stores information about individuals including their full name, work email address (@mail.mil), work phone number, JITC division, branch, and billet, as well as pay amounts charged based on hours entered into DAI. The pay information includes hours worked as entered into DAI as well as the exact cost of those hours (as associated with the employee's rate of pay). Some information is provided when the user's account is created (name, email, and phone) and the remainder is based on DAI report data (division, branch, billet, and pay amounts).

**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)*

The test data that JANETT uses for test and evaluation of system interoperability, including accuracy, completeness, and timeliness of data transactions, must use actual PII or PHI in order to obtain the desired test results.
There are two uses for the real-world data used by the T&E Dashboard. The personal information (name, email, etc.) is for identification purposes and paired with account information for validation of identification.

The financial data provides reporting on JITC employee charges. The intended use is mission-related (programmatic) use to report on government labor charges so that Division Chiefs, Branch Chiefs, and Action Officers can more accurately track their funds. Some of this information will be displayed on a non-individual basis (e.g., exact charges that will be rolled up to the project/branch/division level) and some will be reported along with employee names (hours charged, billet, branch, division, and associated cost).
Additionally, as part of the MRTFB (DoDD 3200.11), and in keeping with its financial regulations (DoD 7000.14-R, "DoD Financial Management Regulation"), JITC is responsible for accurately and efficiently tracking and reporting its financial activities.

**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.

The test data is collected from logs at the enterprise system level to determine the overall systems performance. The approval of individuals is given to the enterprise system, not directly to JITC-FHU. Note, the method used for collection does not allow for isolation or exclusion of records as it would not be representative of the systems environment at the time of test.
The financial analysis information that is collected from DAI is provided via reports produced by Resource Management (RM31) and Office of the Chief Financial Officer (OCFO) personnel. The data includes information from all JITC federal employees utilizing DAI.

**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 are not aware the data is being shared with JITC-FHU for testing. The individual can't object to the general data analysis as the objection would have to be given to the enterprise system.
For the financial analysis data, the Dashboard contains a statement regarding personal data collection when the user requests a Dashboard account and must agree to that statement before proceeding. Individuals cannot access this system without consenting/agreeing to this statement. This would be in regard to information automatically collected as well as that provided to the system on initial request. With respect to the financial information, it is provided as a command initiative and uploaded by select/approved individuals with expressed authority to do so. As this information comes from reports produced from the DAI system, individuals do not have an opportunity to give or withhold consent and the application does not have a way to differentiate data for specific individuals from the reports.

**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

PII is not collected directly from any individual for the testing environment.
For the financial analysis data, a "New User Account Disclaimer" is provided when users request an account explaining that personal information will be collected and that their information will be protected by Dashboard security policy. Text of that statement follows:

"JITC is committed to protecting your privacy and developing technology that gives you the most powerful and safe online experience. This Statement of Privacy applies to the JITC T&E Dashboard and governs data collection and usage. By using the JITC T&E Dashboard, you consent to the data practices described in this statement.

Collection of your Personal Information

JITC T&E Dashboard collects personally identifiable information, such as your e-mail address, name, or telephone number.
There is also information about your computer hardware and software that is automatically collected by JITC T&E Dashboard. This information can include: your IP address, browser type, domain names, access times and referring Web site addresses. This information is used by JITC T&E Dashboard for the operation of the service, to maintain quality of the service, provide audit trails, and to provide general statistics regarding use of the JITC T&E Dashboard.

Use of your Personal Information

JITC T&E Dashboard collects and uses your personal information to operate the JITC T&E Dashboard and deliver the services you have requested.

Security of your Personal Information

JITC T&E Dashboard secures your personal information from unauthorized access, use or disclosure. JITC T&E Dashboard secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information is transmitted it is protected through the use of encryption, such as the Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocol.

Changes to this Statement

JITC T&E Dashboard will occasionally update this Statement of Privacy to reflect company and customer feedback. JITC T&E Dashboard encourages you to periodically review this Statement to be informed of how JITC T&E Dashboard is protecting your information."

**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. JITC-FHU location only. |
| ☐ | 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 | | |

For the testing environment, it varies by test event. Data will be analyzed by JITC-FHU and a report analysis provided to the customer requesting test analysis, but the PII data itself will not be delivered to anyone.
For the financial analysis environment, T&E Dashboard user data and DAI system reports are collected. The user information is collected from individuals and the DAI information comes from an existing DoD Information System.

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

- ☐ E-mail
- ☐ Face-to-Face 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

For the test environment, data will be extracted from the existing information system and transferred to the Test and Development Zone D laptops via DoD SAFE and DVDs, using encryption capabilities, data encrypted at rest, and any folders or databases marked as appropriate. For the financial analysis environment, the data is collected via entry and upload to the T&E Dashboard website. User information is collected from an individual's Common Access Card (CAC) information when they request an account. The rest is collected via report upload to the application.

**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 S890.11 78 FR 65976

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 2.4, Item 010

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

(3) Retention Instructions.

For the test environment, no data is retained. For the financial analysis environment and financial data. Temporary. Destroy 3 years after paying agency or payroll processor validates data, but longer retention is authorized if required for business use. NARA GRS Disposition Authority DAA-GRS-2019-0004-0001.

**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 authorities allow JOINT INTEROPERABILITY TEST COMMAND (JITC) to collect PII/PHI data for testing and/or real-world financial analysis:

- NIST Special Publication 800-122, Guide to Protecting the Confidentiality of PII
- DoD Directive 5400.11, DoD Privacy Program

- 45 CFR 160, 162, and 164, HIPPA Standards for Privacy of Individually Identifiable Health Information
- Privacy Act of 1974 (5 U.S.C. 552a)
- CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP)
- DoD Manual 8910.01, DoD Information Collections Manual: Procedures for DoD Internal Information Collections
- Office of Management and Budget Memorandum M-06-15, “Safeguarding Personally Identifiable Information
- Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of PII

**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 approval is not required in accordance with Section 8.b.11 of Enclosure 3, of DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections." since the public does not log into the system.