PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Interoperability Test Command (JITC) Joint Interoperability Tool (JIT) and WWW Support
DISA Development Business Center Joint Test (DBC JT)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	14689
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.14 - Identity Synchronization Service (IdSS)

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

The following authority allows Joint Interoperability Test Command (JITC) Joint InteroperabilityTool (JIT) and WWW Support to collect the following data:

- 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

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

The JITC Industry Toolkit (formerly named Joint Interoperability Tool) (JIT) is a private web server that is primarily used as an electronic library for JITC products such as Test Reports and Certifications. The JITC Data Management Tool (JDMT) is a web application that resides on the JIT web server. JDMT is comprised of software modules tailored to collect common types of test data used to support test missions. The JDMT is used as a web portal to receive and "pass on" test data files to the Joint Analysis Net Centric Evaluation Testing Toolkit (JANETT) which resides on another server. JDMT will treat all files "passed on" to JANETT as PII & PHI data and will only accept encrypted files, will pass the file to the JANETT server via a network connection to that server, and will immediate delete the file from the JDMT server. JDMT will protect the files per prescribed PII & PHI process. Note: Technically, JIT/JDMT does not collect, maintain, use, or disseminate PII/PHI as allows delivery through its web portal.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Minimal risk of data breach which will be assured by:
1. Access controlled with appointed Memo, System Access Request (DD Form 2875)
2. Required PII & PHI training, Cyber Security awareness training derivative and marking classified course
3. Safety checks EOD to ensure information safeguarded
4. Audit Trail for any access of PII & PHI data
5. Data Encrypted at rest and in transit
6. Data Breach Processes and Procedures in place

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☒ **Other DoD Components.**

Specify. JITC-JTA,JT4 Division(s) test support and instrumentation support teams

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Engility

☐ **Other** (e.g., commercial providers, colleges).

Specify.

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

☐ **Yes** ☒ **No**

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

(2) If "No," state the reason why individuals cannot object.

The agency generating the data based on an individuals' PII/PHI will have the individual sign a privacy act statement to collect the data. The agency working with the system under test program management office will transfer the data to JITC for assessment. While the individual can object to PII/PHI being collected at the agency, once they sign the privacy act statement, they agree to DoD use of that data. Data is collected at the source by the data owner using the system under test and then passed Encrypted by the program management office of the system under test to JITC/JDMT via NIPRNet and CAC login for storage. Data is then accessed via controlled CAC log-in by JITC/JANETT for analysis. In some instances the data files will contain synthetic data created by the program management office for the system under test that need to be treated as PII/PHI for transfer to and storage by JITC.

j. 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.

The agency generating the data based on an individuals' PII/PHI will have the individual sign a privacy act statement to collect the data. The agency working with the system under test program management office will transfer the data to JITC for assessment. While the individual can object to PII/PHI being collected at the agency, once they sign the privacy act statement, they agree to DoD use of that data. Data is collected at the source by the data owner using the system under test and then passed Encrypted by the program management office of the system under test to JITC/JDMT via NIPRNet and CAC login for storage. Data is then accessed via controlled CAC log-in by JITC/JANETT for analysis. In some instances the data files will contain synthetic data created by the program management office for the system under test that need to be treated as PII/PHI for transfer to and storage by JITC.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.	The Privacy Act of 1974, 5 USC 552a, provides protection to individuals by ensuring that personal information collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy. Pursuant to 5 U.S.C. §552a (e) (3) agencies are required to provide what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number). Department of Homeland Security (DHS) policy is to provide a Privacy Act Statement regardless of whether the collection is part of a system of records or not. All Privacy Act statements must be reviewed by the Privacy Office or component Privacy Officer. When drafting a Privacy Act Statement for review by the Privacy Office, include the following elements: • Authority: The legal authority for collecting the information – statute, executive order, regulation. • Purpose: The purpose(s) for collecting the information and how DHS will use it. • Routine Uses: To whom DHS may disclose the information outside of the Department and for what purposes. • Disclosure: Mandatory or Voluntary: Whether providing the information is mandatory or voluntary. DHS can only make collection mandatory when a Federal statute, executive order, regulation, or other lawful order specifically imposes a duty on the person to provide the information; and the person is subject to a specific penalty for failing to provide the requested information. The effects, if any, of not providing the information – for example the loss or denial of a privilege, benefit, or entitlement sought as a consequence of not furnishing the requested information.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.