



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the [DOI PIA Guide](#) for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Drug Testing System Provider (DTS-P)

Bureau/Office: Office of the Secretary/Interior Business Center

Date: September 30, 2021

Point of Contact

Title: OS Departmental Offices Associate Privacy Officer

Name: Danna Mingo

Phone: 202-441-5504

Email: OS_Privacy@ios.doi.gov

Address: 1849C Street, NW Room 7112 Washington DC 20240

Section 1. General System Information

A. Is a full PIA required?

- Yes, information is collected from or maintained on
- Members of the general public
 - Federal personnel and/or Federal contractors
 - Volunteers
 - All

No:

B. What is the purpose of the system?

The U.S. Omnibus Transportation Employee Testing Act of 1991 requires drug and alcohol testing of safety-sensitive transportation employees in aviation, trucking, railroads, mass transit, pipelines, and other safety-sensitive positions. Executive Order 12564 requires Executive Branch Agencies to have a Drug-Free Workplace Plan and drug test employees and applicants. Department of Health and Human Services (HHS) Mandatory Guidelines for Federal Drug Testing Programs (HHS Mandatory Guidelines) effective on October 1, 2017



permit the utilization of pre-employment and periodic random testing for Federal employees in sensitive positions. According to the HHS Mandatory Guidelines, Federal employees may also be tested on the basis of reasonable suspicion of drug use and during post-accident and follow-up testing after the employee has completed a rehabilitation program.

The Drug Testing System – Provider (DTS-P) is a web-enabled system that allows the Government to execute the Drug-Free Workplace Program with an internet-based application. DTS-P streamlines the process for submitting requests, expediting the posting of results, reduces data entry errors from request forms, and provides the current status for all drug and alcohol tests. Federal agency customers can use DTS-P to schedule drug/alcohol tests, track test status, and report test results for Federal government employees and prospective employees in accordance with HHS and Department of Transportation (DOT) regulations.

DTS-P is owned, hosted, and maintained by Pembroke Occupational Health, a Department of the Interior (DOI) contractor, who provides the system as a Software as a Service (SaaS) and uses Unitas Global as a hosting facility through a Sub-Business Associate Agreement. DOI uses DTS-P for DOI employees and prospective employees who are subject to drug testing. DTS-P is also offered by the DOI Interior Business Center (IBC) as a shared service provider to Federal agency customers for use on a payfor service basis. DOI oversees the DTS-P by maintaining the contract and ensuring that privacy and security controls are in place and that the system has been certified and accredited. DOI facilitates Federal agency user access to the DTS-P application by coordinating and approving user account requests before the requests are forwarded to the vendor for creation.

C. What is the legal authority?

Executive Order 12564, Drug-free Federal Workplace; the Omnibus Transportation Employee Testing Act of 1991; 49 CFR Part 40, Procedures for Transportation Workplace Drug and Alcohol Testing Programs; HHS Mandatory Guidelines for Federal Workplace Drug Testing Programs (HHS Mandatory Guidelines effective on October 1, 2017); 5 U.S.C. § 7301, Presidential Regulations; and 5 U.S. Code § 3301 - Civil service

D. Why is this PIA being completed or modified?

- New Information System
- New Electronic Collection
- Existing Information System under Periodic Review
- Merging of Systems
- Significantly Modified Information System
- Conversion from Paper to Electronic Records
- Retiring or Decommissioning a System
- Other:



E. Is this information system registered in CSAM?

Yes:

UII Code: 010-999991241, SSP Name: Drug Testing System – Provider

No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII	Describe
DTS-IBC	DOI/Customer Responsibilities	Yes	DTS is a web-enabled system operated by Abbott eScreen that allows DOI and client federal agencies (users) to schedule a drug/alcohol test, track the status, and report the results for testing as required in accordance with the Department of Health and Human Services DHHS and the Department of Transportation (DOT) regulations.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

Yes:

Records pertaining to or resulting from the testing of employees for use of illegal drugs are maintained under government-wide system of records notice, OPM/GOVT-10 - Employee Medical File System Records, 75 FR 35099 (June 21, 2010); modification published at 80 FR 74815 (November 30, 2015). Records related to an applicant's examination for use of illegal drugs are maintained under government-wide system of records notice, OPM/GOVT-5 - Recruiting, Examining and Placement Records, 79 FR 16834 (March 26, 2014); modification published at 80 FR 74815 (November 30, 2015). These notices may be viewed on the DOI SORN page at <https://www.doi.gov/privacy/sorn>.

No



H. Does this information system or electronic collection require an OMB Control Number?

Yes:

There are two Federal forms are used to collect information for this system:

- Federal Drug Testing Custody and Control Form, OMB No. 0930-0158, Expiration Date: 8/31/2023
- U.S. Department of Transportation (DOT) Alcohol Testing Form (DOT F1380), OMB No. 2105-0529, Expiration Date: 12/31/2023

No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

- Name
- Gender
- Birth Date
- Social Security Number (SSN)
- Truncated SSN
- Personal Cell Telephone Number
- Home Telephone Number
- Employment Information
- Other:

Employee ID, duty location, and the information related to the required tests, such as the testing result, the specimen number, type of test (pre-employment, random, reasonable suspicion, reasonable cause, post-accident, follow-up) drug and/or alcohol test (including results of urinalysis, oral fluids, breath test), collection date, collection city and state, and clinic number of the test of the employees and applicants tested in accordance with HHS Guidelines and DOT regulations are processed by DTS-P. DTS-P also records and stores information related a specific test such as test mode, tested for status; date selected, status, reason (i.e., TDY; furlough; etc.).

B. What is the source for the PII collected? Indicate all that apply.

- Individual
- Federal agency
- Tribal agency
- Local agency
- DOI records
- Third party source



- State agency
- Other:

The information recorded in DTS-P includes DOI, other Federal agency customers, the Collection/Medical Review Officer Contractor, and the Laboratory Contractor from whom the PII is recorded.

C. How will the information be collected? Indicate all that apply.

- Paper Format
- Email
- Face-to-Face Contact
- Web site
- Fax
- Telephone Interview
- Information Shared Between Systems Describe
- Other:

Information about current DOI and some Federal customer employees is obtained from the DOI Federal Personnel and Payroll System (FPPS), or the human resources or personnel systems of other Federal agencies and is manually entered by the DTS-P users. Users are typically Human Resources staff at DOI or one of IBC's customer agencies.

Information on prospective employees is obtained from the servicing personnel officers. This information includes name, full or partial Social Security number (SSN), contact telephone number (home or cellular), gender, and city and state of residence.

Due to statutory chain of custody requirements, the scheduling, specimen collection, and Medical Review Officer (MRO) requirement (Collection & MRO) must be provided under a separate contract. Lab result information is obtained from a third-party testing lab. Review and analysis of results is provided by the Medical Review Officer (MRO). DTS-P imports data from the laboratory and MRO and serves as a central location for authorized users to obtain all test results and related information.

At the time of the specimen collection, the donors/employees also provide their date of birth, day, and evening phone number.

D. What is the intended use of the PII collected?

The data is used to track and report the drug test status and results of the existing and prospective federal employees. Results from testing employees for use of illegal drugs or the illegal use of licit drugs, including negative results, confirmed or unconfirmed positive test results, and information related to the reasons for testing, may be used for personnel actions; referrals to the Employee Assistance Program or rehabilitation programs; administrative,



disciplinary or adverse actions; and to comply with Federal law, regulations, policy. Records related to an applicant's examination for use of illegal drugs or the illegal use of licit drugs may be used in suitability determinations for employment in accordance with E.O. 12564 and the Omnibus Transportation Testing Act of 1991.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

Within the Bureau/Office:

DOI Drug & Alcohol Testing Branch Staff will use the data to track the drug test status and results of the existing and prospective Federal employees of DOI.

Other Bureaus/Offices:

DOI Drug & Alcohol Testing Branch Staff will share the testing results with the corresponding bureaus that order the tests.

Other Federal Agencies:

The data is used to track the drug test status and results of the existing and prospective Federal employees of other Federal agency customers who access the application as a web-based service. After logging on to DTS-P, the Federal customers' Federal Drug Screening Managers can schedule an alcohol and/or specimen collection, and review the final result determined by the MRO. Each Federal DTS-P user is permitted to see only data specific to its agency or subcomponent. Results of a drug test may be disclosed pursuant to an order of a court of competent jurisdiction where required by the United States Government to defend against any challenge against any adverse personnel action as permitted under routine uses outlined in the OPM/GOVT-10 and OPM/GOVT-5 system of records notices.

Tribal, State or Local Agencies:

Contractor:

DOI contractors have access to the data in DTS-P. Pembroke Occupational Health has access to data in DTS-P as the system operator to host the system, perform system updates, and manage drug testing program functions in the system. Contracted DTS-P administrators and developers administer and maintain the system at the outsourced data center. The designated Government Contract Drug Testing Laboratory contractor is responsible for providing data to DTS-P. The Collection/MRO contractor has access to test results. The contractor is required not to release any records or information relating to participating agency programs or employees without the advance written approval of the agency contract representative (COR).



Other Third-Party Sources:

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Yes:

Individuals may decline to provide information as submission of information on the Custody and Control form or during the drug testing process is voluntary. However, incomplete submission of information may result in delay or denial of employment application or removal from the Federal service or other disciplinary action. An alternative number will be provided if the individual does not want to provide an SSN.

No:

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

Privacy Act Statement:

A Privacy Act statement is provided on the FEDERAL DRUG TESTING CUSTODY AND CONTROL FORM.

Privacy Act Statement: (For Federal Employees Only) Submission of the information on the attached form is voluntary. However, incomplete submission of the information, refusal to provide a urine specimen, or substitution or adulteration of a specimen may result in delay or denial of your application for employment/appointment or may result in removal from the Federal service or other disciplinary action. The authority for obtaining the urine specimen and identifying information contained herein is Executive Order 12564 ("Drug-Free Federal Workplace"), 5 U.S.C. Sec. 3301 (2), 5 U.S.C. Sec. 7301, and Section 503 of Public Law 100-71, 5 U.S.C. Sec.7301 note. Under provisions of Executive Order 12564 and 5 U.S.C. 7301, testresults may only be disclosed to agency officials on a need-to-know basis. This may include the agency medical review officer, the administrator of the Employee Assistance Program, and a supervisor with authority to take adverse personnel action. This information may also be disclosed to a court where necessary to defend against a challenge to an adverse personnel action. Submission of your SSN is not required by law and is voluntary. Your refusal to furnish your number will not result in the denial of any right, benefit, or privilege provided by law. Your SSN is solicited, pursuant to Executive Order 9397, for purposes of associating information in agency files relating to you and for purposes of identifying the specimen provided for testing. If you refuse to indicate your SSN, a substitute number or other identifier will be assigned, as required, to process the specimen.



Privacy Notice:

Notice is provided through the publication of this privacy impact assessment and the government-wide system of records notices OPM/GOVT-10 - Employee Medical File System Records, and OPM/GOVT-5 - Recruiting, Examining and Placement Records, which may be viewed at <https://www.doi.gov/privacy/sorn>.

Other:

None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc. .

Data can be retrieved using several search fields: last name, truncated SSN, Custody and Control Form Number or Date.

I. Will reports be produced on individuals?

Yes:

Reports on the results or status of drug tests of persons required to take the tests are produced and are used to schedule or track drug and alcohol results. Users who have access to an agency's drug test results/records can access these reports.

No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data that is manually entered into DTS-P is verified by the DTS-P users who are either the HR representative or Drug Program Coordinator of the Federal agency data owner with access right to verified information about employees or prospective employees. At the time of the collection, the employees/prospective employees provide information such as their truncated SSN, phone number, full name, and DOB and have the opportunity to verify their previously provided information such as their truncated SSN and full name for accuracy. If mistakes are found in DTS-P after these events, the users of the system can make corrections.

B. How will data be checked for completeness?

Each agency using DTS-P is responsible for ensuring the data is complete. Those entities who originally enter the PII may update the data to ensure the completeness.



C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The collection contractors regularly update the donor record and update the Date-Of-Last-Action-On-Donor-Record on the Donor record whenever they receive the data so the new information will be sent to the requesting Federal office when the office logs on the internet-based application. There is a process that checks and corrects error for those records that are sent in error. When an error is detected, the collection contractor sends the record back to the laboratory contractor with an additional field identifying the error(s) found. The laboratory contractor is responsible for correcting and re-transmitting the record.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

DOI records in DTS-P are maintained under Department Record Schedule (DRS) - 1, Short-term Human Resources Records (DAA-0048-2013-0001.0004), which was approved by the National Archives and Records Administration (NARA). This records schedule covers Federal Workplace Drug Testing Program Files, including all the files categorized as drug test plans and procedures, selection/scheduling records, records concerning the collection and handling of specimens, and test results. The disposition is temporary. The cut-off of record starts as instructed in the agency/bureau records manual, or at the end of the fiscal year in which the record is created if no unique cut-off is specified. The records are destroyed three years after cut-off.

Some records related to specific drug testing and results may require different retention by the DTS-P contractor in accordance with the latest version of HHS guidelines, DOT regulations, or records retention schedule promulgated by NARA.

Each Federal agency customer is the data owner for their records in DTS and is responsible for maintaining their records in accordance with the Federal Records Act.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

DOI approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

The DTS-P records will be destroyed by pulping, macerating, shredding or by otherwise definitively destroying the information contained in the records in accordance with 36 CFR 1228.58. Destruction shall be witnessed by a contractor employee.

Federal agency customers' electronic records will be destroyed in accordance with Federal regulations, as approved in advance by each Federal agency.



F. Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals as DTS-P collects, processes, and stores sensitive PII. The privacy risks are mitigated by the corresponding measures implemented to ensure PII is collected for specific legitimate purposes via transparent and fair notice and consent process, shared with regulatorily authorized entities, stored and disposed according to approved Federal records retention schedules and procedures, and sufficiently safeguarded to protect privacy. DTS-P has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. DTS-P is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

Purpose of data collection: DOI ensures that the data collected and processed by DTS-P is necessary to perform those functions as specified and required by the related Federal Executive Orders, laws, and regulations. The PII is collected only from Federal employees and prospective employees (data subjects) who are subject to drug testing and will only be used to meet the specified Federal regulatory requirements.

Consent and Notice: PII is collected from the data subject through proper notice and consent process and the data fields are strictly prescribed by Federal regulations and guidelines and are standardized. The submission of the PII is voluntary. The data subject has the option to decline the tests and not to provide their personal information should they choose not to pursue the job opportunity. The data subject also has the option to use an alternative identifier should they choose not to use their SSN as their unique identifier. A Privacy Act Statement in the Federal Drug Testing Custody and Control Form unambiguously notifies the data subjects of their right and options.

Disclosure, Retention and Disposal: There is a risk that individuals may gain unauthorized access to the information or users will conduct unauthorized activities such as using, extracting, and sharing information with unauthorized recipients. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties. The PII collected, processed and stored in DTS-P can only be accessed by the authorized certified professionals who provide lab services or lab result evaluation service and the designated personnel of the Federal agency employers who order the service per specific permission by relevant guidance and regulations. There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Only the minimal amount of data needed to implement the Drug-Free Workplace Program and track drug test status and results of the existing and prospective Federal employees is maintained and used by the system. DOI DTS-P records will be retained according to DOI records retention schedule approved by



NARA and will be disposed of in accordance with NARA guidelines and Departmental policy. The publication of this PIA, and applicable government-wide system of records notices provide contact information and procedures for data subjects to request information.

Safeguards of PII: The Contractor has ensured that information security considerations have been included in everything from network design to account management, and the DTS-P access permissions are segregated and restricted between each environment based on required job responsibilities. Role based security is employed to restrict user functions when using the applications and the access is reviewed on a regular basis to re-validate non-standard access rights. The DTS-P data in transit and at rest are encrypted. Administratively, the Contractor provides their employees with security awareness training annually, which is tracked and monitored based on Contractor corporate policies and procedures. Contract employees are mandated to read and sign the Employee Handbook, which contains the IT rules of behavior for Contractor systems. The Contractor has as a Social Media Policy in its Employee Handbook outlining the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. Each employee must sign an acknowledgement of receipt at time of hire or major revision of the Employee Handbook. The Contractor will continue to maintain the established formal process without deviation.

The DTS-P system is accessed through the Internet via HTTP Secure, which provides an encryption layer to prevent unauthorized access over the Web and ensures secure transmission of information. The contract between DOI and the service providers set strict requirements on the administrative, technical and physical controls that the contractors must put in place to maintain the confidentiality, integrity and availability of the PII and the test information and ensure all therecords are maintained and used with highest regard for privacy. In addition, all DOI employeesand contractors are required to take the annual privacy and security training and acknowledge rules of behavior prior to being issued or renewed a user account.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes:

The purpose of the system is for scheduling, tracking, and reporting the results of drug/alcohol tests for Federal government employees and prospective employees in accordance with the HHS and DOT regulations. The use of the data is both relevant and necessary for this purpose.

No



B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Yes:

No

C. Will the new data be placed in the individual's record?

Yes:

No

D. Can the system make determinations about individuals that would not be possible without the new data?

Yes:

No

E. How will the new data be verified for relevance and accuracy?

Not applicable, this system does not create new data.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated.

Yes, processes are being consolidated.

No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

Users

Contractors

Developers

System Administrator

Other: *Describe*

Personnel who have access to the data in DTS-P are authorized Federal agency personnel (typically drug program managers and their support staff), DOI drug program personnel and servicing personnel officers, and contractor (system administrators and support staff).



A separate vendor (Quest Diagnostics) provides laboratory services and transmits these results to the vendor using their Laboratory Information Management System. The lab vendor does not have access to DTS, or the data contained within DTS-P but provides a new set of data (the drug test result) which ultimately is posted in DTS-P.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Each agency identifies authorized users on a strict need-to-know basis. Authorized users are granted access via ID and password and user activities are tracked via audit trail.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

Yes.

The application was designed and developed by the DOI Contractor, who hosts the system, performs system updates, and operates and manages the system. Privacy Act contract clauses were included in the contract.

No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

Yes.

No

K. Will this system provide the capability to identify, locate and monitor individuals?

Yes.

No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system does not have the ability to identify, locate and monitor individuals. The system does contain an audit log that can be used to review the actions of users accessing the system. This information includes user identification, time of access, and the list of files and data elements accessed.



M. What controls will be used to prevent unauthorized monitoring?

Access to the system is restricted to authorized personnel with valid user IDs and passwords. User accounts allow authorized personnel to only access the data for their agency or department. The DTS-P system is accessed through the Internet via HTTP Secure, which provides an encryption layer to prevent unauthorized access over the Web. The audit log tracks the user's last login date and time, and the number of login attempts.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- Security Guards
- Key Guards
- Locked File Cabinets
- Secured Facility
- Closed Circuit Television
- Cipher Locks
- Identification Badges
- Safes
- Combination Locks
- Locked Offices
- Other.

(2) Technical Controls. Indicate all that apply.

- Password
- Firewall
- Encryption
- User Identification
- Biometrics
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- Public Key Infrastructure (PKI) Certificates
- Personal Identity Verification (PIV) Card
- Other.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Backups Secured Off-site
- Rules of Behavior
- Role-Based Training
- Regular Monitoring of Users' Security Practices



- Methods to Ensure Only Authorized Personnel Have Access to PII
- Encryption of Backups Containing Sensitive Data
- Mandatory Security, Privacy and Records Management Training
- Other.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The DTS-P Information System Owner is the official responsible for oversight and management of the DTS-P security controls and protection of information processed and stored by the DTS-P system. The Information System Owner, Information System Security Officer, and the DTS-P Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy and providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with DOI Privacy Officials. These officials and authorized DTS-P personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act and other Federal laws and policies for the data managed, used, and stored in DTS-P.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The DTS-P Information System Owner is responsible for oversight and management of the DTS-P security and privacy controls, and for ensuring to the greatest possible extent that DOI and customer agency data in DTS-P is properly managed and that access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to DOI-CIRC within one hour of discovery, as well as the Federal customer agency, in accordance with Federal policy and established procedures. Customer agency data in DTS-P is under the control of the customer agency. Each customer agency is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access, or disclosure of data resulting from their activities, processing, or management of the data.