U.S. Department of Transportation

Privacy Impact Assessment
Office of the Secretary of Transportation (OST)

Drug and Alcohol Testing Management System (DATMIS)

Responsible Official

Tonya Templeton
Manager
Substance Abuse Awareness Testing Office (SAATO)
Tonya.Templeton@dot.gov

Reviewing Official

Karyn Gorman
Chief Privacy
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Department of Transportation (DOT) Substance Abuse Awareness Training Office (SAATO) administers drug and alcohol testing to DOT employees and employees of other federal agencies. SAATO is under Workforce Quality within the DOT Office of Human Resource Management. The Drug Alcohol Testing Management Information System (DATMIS) is a DOT application used to randomly select DOT employees and employees from other agencies with who they have agreements within safety or security sensitive positions for drug and alcohol testing. DATMIS is a secure-web-application-owned and used only by the SAATO to also to record and store the results of drug testing. Drug and alcohol testing is mandated by E.O. 12564, Drug-Free Federal Workplace; 49 CFR Part 40, Procedures for Transportation Workplace Drug and Alcohol Testing Programs Omnibus Transportation Act, Employee Testing Act of 1991, and collects and maintains Social Security Numbers (SSN), E.O. 9397, SSN as amended. These functions carried out through DATMIS are in accordance with Executive Order 12564, the Omnibus Employee Testing Act of 1991, and DOT Order 3910.1D, Drug and Alcohol-Free Departmental Workplace Program, OPM/GOVT-10, Employee Medical File System Records, and the Health and Human Service (HHS) Mandatory Guidelines for Federal Drug Workplace Programs.

DATMIS is not publicly available and does not solicit information from members of the public, but data maintained in the system contains Personally Identifiable Information (PII) and as such, this Privacy Impact Assessment is being updated[1] as required by the E-Government Act of 2002.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and iii) examine and

[1] Previous version of DATMIS PIA can be found here.

evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[2]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

DATMIS is a departmental application owned and used only by SAATO. SAATO provides drug and alcohol testing services for DOT employees, the U.S. Merchant Marine Academy (USMMA), and Department of Homeland Security (DHS) agencies to include the Transportation Security Administration (TSA), Federal Air Marshals (FAM), and U.S. Coast Guard (USCG), through inter-agency agreements. The system generates monthly random test lists for safety or security sensitive employees from personnel data files for DOT including USMAA, as well as TSA, FAM, and USCG.

There are three procedures DATMIS uses to complete the drug and alcohol testing process that include (1) random selection, (2) test results storage and records maintenance; and (3) follow-up testing scheduling. Historical drug test results for random, pre-employment, reasonable suspicion, post-accident/post-incident, return-to-duty, and follow-up testing are stored in DATMIS. Follow-up testing scheduling records for employees in a rehabilitation program are also maintained.

For DOT employees, DATMIS ingests a Federal Personnel and Payroll System (FPPS) extract data file via server connection to schedule the periodic random drug and alcohol

[2]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

testing as mandated by federal laws and policies. Other participating agencies that use this service send PII data to SAATO using a secure and encrypted method. The personnel data file contains names, SSNs, duty locations, drug and alcohol test codes, and the sex of employees in the drug and alcohol testing program. Data is automatically uploaded through an encrypted interface into DATMIS to maintain an accurate record of employees in these positions. Personnel data is refreshed in DATMIS depending on the organization providing the data. This process helps ensure only this data is used to randomly select employees for testing who are currently in a safe or security sensitive positions. A profile for all employees in a safety or security sensitive position is created in the personal data file that is used to match employee test results for the purpose of storing historical testing records. DATMIS's three functions are further outlined below.

RANDOM SELECTION PROCESS

The DOT random testing method is designed to ensure all employees in a safety or security sensitive positions are subject to random identification on a statistically equal basis with respect to their duty location. Identification of employees selected for random testing is accomplished by using a computer draw from DATMIS. The computer draw has all employees in one pool. The selection process is completed for each Department that we service separately. SAATO manages the selection process and random selection of employees. This is done to ensure there are no opportunities for any employee to influence the selection/non-selection of employees for testing. Identifying duty locations of the employees is the first step in structing the random identification of the employees. A preset percentage of the employees on the test lists will be tested within any given scheduled day. Testing begins with the first name on the test list and moves sequentially down the list. If the employee is on pre-approved annual or sick leave, or is unavailable for any legitimate reason, e.g., off-site training, at the time of testing, he or she will not be tested. The random list is annotated to indicate the reason for an employee not being available. The annotated lists become official documentation of the sequence of testing, and these are returned to SAATO through the Drug Program Coordinator (DPC) and retained for audit purposes. Testing is completed when the preset percentage of testing is achieved, or the bottom of the list is reached, whichever comes first. A Federal Drug Chain of Custody Form (CCF) or DOT Breath and Alcohol Test Form (BATF) is used to document the employee's testing process. These documents are stored in SAATO in a secure location for three years in accordance with OPM/GOVT-10, Employee Medical File System Records.

TEST RESULTS STORAGE AND RECORDS MAINTENANCE

During drug testing, employees complete and sign a CCF to ensure proper identification and tracking of their sample. The test is done through urinalysis using a split specimen collection,

where the sample is divided into two containers. The primary sample is tested, and the split sample is stored as a backup.

Testing is conducted by Department of Health and Human Services (HHS) certified labs, which follow strict quality controls. The labs perform an initial drug screening and confirm results if necessary. If a drug test is positive, a Medical Review Officer (MRO) contacts the employee to check for any valid medical explanation.

Drug test results from HHS-certified laboratories are securely sent to SAATO using a File Transfer Protocol (FTP) connection. SAATO downloads these results into DATMIS.

If an employee used their SSN during testing, DATMIS automatically matches the test results to their employee profile. If the employee did not use their SSN, the test result can still be identified using the CCF number and the employee's name on the form, but it will not be linked to their profile in DATMIS.

Test results for random, pre-employment, reasonable suspicion, post-accident/post-incident, return-to-duty, and follow-up testing are matched to the employee's personnel records when possible. These records are securely stored in compliance with OPM/GOVT-10 guidelines. Alcohol testing is conducted using an evidential breath-testing device approved by the National Highway Traffic Safety Administration (NHTSA). A DOT-certified contract breath-alcohol technician (BAT) performs the testing.

The process starts with a screening test**.** If the result is 0.02 or higher, or 0.01 or higher during follow-up testing, a confirmation test is conducted 15 minutes later. The confirmation test result determines any further action.

The site coordinator (a federal employee) is provided a test list that includes employees' **SSNs** to identify the correct individuals for testing. The collector does not have access to any PII such as SSNs. Instead, the collector uses the employee's government-issued ID to confirm their identity before testing.

All tests are handled with respect for confidentiality, safety, and security. Alcohol test results are not stored in the DATMIS system. Any printed drug and alcohol test results are kept in a secure location with access strictly limited to authorized personnel on a need-to-know basis. The secure storage complies with DOT standards for protecting sensitive PII.

FOLLOW-UP TESTING SCHEDULING

DATMIS keeps records of follow-up testing schedules for employees in a rehabilitation program. To start the follow-up scheduling process, SAATO receives a copy of the employee's return-to-duty (RTD) test (CCF) and/or DOT Breath Alcohol Test Form (BATF) by a secured method. A folder is created for each new employee in the program. The employee's agency then sends a follow-up worksheet, through a secure method, when the employee is ready for the follow-up program.

After SAATO receives the worksheet, an email request is sent to the scheduling contractor, a federal contract employee, to assign a collector for the employee. The collector assignment provides the contact details and testing location of the assigned collector. The employee's information is then entered into the DATMIS system, including their name, SSN, date of birth, sex, duty location, operating administration, Drug Program Coordinator (DPC), collector details, and testing frequency.

Each month, DATMIS generates follow-up testing lists, which are sent by email to the relevant field DPC, agency contact, and collection contractor. Testing is then arranged and completed. Follow-up testing records are stored securely, in accordance with OPM/Govt-10 guidelines, and follow the same procedures as other test records.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[3], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

The Privacy Act of 1974, as amended, requires System of Records Notices (SORN) for all systems (electronic or paper) where information is retrieved using a personnel identifier. The DOT provides general notice to the public of this records collection through the Privacy Act system of records notice (SORN), OPM/GOVT-10-Employee Medical File System Records, June 21, 2020, 75 FR 35099, which provides general knowledge to the public. Records may be retrieved by the employee's name, date of birth, SSN, or any combination of those

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

identifiers. There are no exemptions claimed for the system. Information is this system may be shared outside of OPM with the exception of Routine Use ‘‘u,’’ none of the other Routine Uses identified for this system of records are applicable to records relating to drug testing under Executive Order 12564. Further, such records shall be disclosed only to a very limited number of officials within the agency, generally only to the agency Medical Review Official (MRO), the administrator of the agency Employee Assistance Program, and the management official empowered to recommend or take adverse action affecting the individual. A comprehensive list of routine uses may be found in the System of Records Notice OPM/GOVT-10.

When an individual accepts a safety or security sensitive position, they are notified with a pre-employment letter that states they are subject to drug and/or alcohol testing. When an employee is tested, they receive the Health and Human Services – Substance Abuse and Mental Health Administration (HHS-SAMHSA) Federal Chain-of-Custody (CCF) form that includes a Privacy Act Statement. Consent is not required for test administration. A signed statement must be provided by the employee before their information can be released beyond SAATO. The following forms are used in this process.

HHS-SAMHSA, Federal Drug Testing Chain-of-Custody (CCF) form OMB# 0930-0158 collects employees names and if they choose to provide it, the employees SSN. The purpose of collecting employees PII is to accurately identify the employee to the test result.

The DOT Federal Alcohol Testing Form, OMB#2105-0529 is used to collect employees names and if they choose to provide it, the employee’s SSN. The purpose of collecting employees PII is accurately identify the employee to the test result.

The publication of this PIA further demonstrates the DOT Office of Human Resource Management, commitment to provide appropriate transparency for the DATMIS SAATO.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Individuals that accept a safety or security sensitive position are notified with a pre-employment letter that states they are subject to drug and/or alcohol testing. Information is collected directly from the employee on the Federal CCF and DOT BATF at the time of testing. Employees who complete the form are responsible for the accuracy of the PII information they must provide at the time of testing. A Privacy Act Statement (PAS) is on the Federal CCF form. Consent is not required for test administration. A signed statement

must be provided by the employee before their information can be released beyond SAATO. However, throughout the remaining drug and alcohol testing process, the employee has the right to deny providing their SSN. If an employee chooses not to provide their SSN there is no penalty assessed on the employee. SAATO is not allowed to use the data for any other reasons beyond drug and alcohol testing.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of DATMIS to determine if any records have been added that may pertain to them. The Freedom of Information Act (FOIA) is a federal law that gives individuals the right to access any DOT records unless DOT reasonably foresees that the release of the information in those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. The DOT will review all Privacy Act requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Current and previous employees from DOT and the other agencies Department of Homeland Security, TSA, FAM, USCG and USMMA should submit their request to SAATO.

Notification procedure: Individuals wishing to know if their records appear in this system may inquire in writing to the appropriate system manager. When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 49 CFR part 10.

You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

Department policy requires the inquiry to include the name of the individual, mailing address, phone number or email address, a description of the records sought, and if possible, the agency and location of the records. If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Tonya Templeton (System Manager)
Substance Abuse and Awareness Testing Office (M-14.3)
1200 New Jersey Avenue, S.E.
Washington, DC 20590
Tonya.templeton@dot.gov
(202) 366-0798

Contesting record procedures: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for

why the records should be corrected. Refer to the Notification Procedures section for additional requirements. Requests should be submitted to the attention of the OST official responsible for the record at the address below:

Tonya Templeton (System Manager)
Substance Abuse and Awareness Testing Office (M-14.3)
1200 New Jersey Avenue, S.E.
Washington, DC 20590
Tonya.templeton@dot.gov
(202) 366-0798

Additional information about the Department's privacy program may be found at DOT Privacy Program | US Department of Transportation. Individuals may also contact the DOT Chief Privacy Officer at privacy@dot.gov.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

The purpose of the system is to accurately identify employees in safety or security sensitive positions required and selected for random drug and alcohol tests. DATMIS is also used to record and store the results of drug testing for random, pre-employment, reasonable suspicion, post-accident/post-incident, return-to-duty, and follow-ups. Federal agencies that participate in the program besides DOT include DHS agencies TSA, FAM, and USCG and employees in safety or security sensitive positions. Employees in safety and sensitive positions are required by Executive Order 12564, Omnibus Employee Testing Act of 1991 (this applies to FAA employees and commercial driver's license holders only), DOT Order 3910.1D, and the HHS Mandatory Guidelines to participate in random drug and alcohol testing. In addition, the system provides historical records in accordance with OPM/GOVT-10, Employee Medical File System Records June 19, 2006, 71 FR 35360. Information maintained and collected are only used for the purpose for which it is collected and outlined in OPM/GOVT-10.

DATMIS is integral to the operation of the drug and alcohol testing program responsibly to ensure safety of the transportation system in accordance with the Executive Order 12564 and the Omnibus Transportation Act of 1991.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

DATMIS only collects and uses the minimum necessary PII to generate monthly random test lists for DOT employees in safety or security sensitive positions from the FPPS. The minimum necessary PII is received, collected, and used for this requirement as well for DHS federal agencies (TSA, FAM, USCG) that participate in this program. The system stores statistical data of drug test results for random, pre-employment, reasonable suspicion, post-accident/post-incident, return-to-duty, and follow-up testing and maintains follow-up testing scheduling records for employees in a rehabilitation program.

Data is retained in the system for 3 years in its unaltered state as received from DOT FPPS and data files received from additional agencies, and testing records/results are maintained in the system for three years in accordance OPM/GOVT - 10, Employee Medical File System Records, June 21, 2010, 75 FR 35099 in accordance with the following record schedule:

General Record Schedule (GRS), 2.7, Employee Health and Safety Records:

- *Item 130*, Employee drug test results, DAA-GRS-2017-0010-0019, Temporary. Destroy when employee leaves the agency or when 3 years old, whichever is later; and
- *Item 131*, Exclusion, DAA-GRS-2017-0010-0020, Temporary. Destroy when 3 years old.

GRS 5.2, Transitory and Intermediary Records:

- *Item 020,* Intermediary Records, DAA-GRS-2022-0009-0002, FPPS data file and USCG, TSA/FAM data. Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

All hard copies of drug and alcohol test information required by the records, retention, and maintenance are stored in a secure location. Only authorized SAATO employees have access to the secure data. All hard copies three or more years old are disposed of in accordance with the records retention requirements outlined in the OPM/GOVT – 10. Electronic drug and alcohol test information is purged out of the DATMIS system.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

DATMIS collects PII and this information is not used in any manner that is not specified in the system of records notices. Data is only used to generate monthly random test lists for safety or security sensitive employees working for DOT or other federal agencies. The system receives data files from the DOT FPPS for DOT employees only, and encrypted data files from the DHS agencies TSA, FAM, USCG and USMMA, and stores statistical data of

drug test results for random, pre-employment, reasonable suspicion, post-accident/post-incident, return-to-duty, and follow-up testing and maintaining follow-up testing scheduling records for employees in a rehabilitation program.

The DATMIS system is only used by SAATO employees. SAATO employees complete DATMIS rules and behavior and security awareness training to ensure employees know the responsibilities on using PII annually. DATMIS does not publicly post any PII information. The only agencies outside of DOT we share DATMIS data with is TSA, FAM, USCG. This data sharing process occurs in accordance with an Inter-agency Agreement (IA) between the agencies.

Records in the system are covered, maintained, and used in accordance with OPM/GOVT - 10, Employee Medical File System Records June 10, 2010, 75 FR 35099. Records may be disclosed outside of OPM as described in the published notice. There are no exemptions claimed for the system.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Data in DATMIS is not updated manually, but provided via a linked server encrypted connection to ensure the data received is as accurate. Personnel data is provided by the employee on the CCF for the drug testing procedure purposes only. As such, authorized personnel manually verify and enter the proper data provided on the CCF minimizing data entry and integrity issues in the system. Data received from the laboratory files cannot be edited by staff members. SAATO employees conduct quality control checks of all paperwork to ensure the PII is accurate on a daily basis. Ff changes are required, the laboratory makes the corrections and resends the data.

To preserve quality and integrity if data in the system becomes corrupt or needs to be restored, differential system backups are done on a regular basis and a full backup is performed often. OST ensures the collection, use, and maintenance of information collected for operating DATMIS is relevant to the purposes for which it is to be used and to the extent necessary for those purposes, it is accurate, complete, and up to date. The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of information.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure,

as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

DATMIS takes appropriate security measures to safeguard PII and other sensitive data. DOT security standards are applied to the system, including but not limited to routine scans and monitoring, back-up activities, and background security checks of OST employees and contractors.

The system is not accessible to the public; it can only be accessed through the DOT network. This server is behind the DOT firewall as it is meant for internal use only. The DOT network has been designed for ultimate protection from internet attacks and there are protective devices strategically placed to prevent unwanted attacks from within the network. Intrusion detection/prevention and firewall devices are deployed throughout the network to protect the network from many of the malicious codes.

Only authorized users have access to the system. Before employees can obtain access to the system, they must sign a non-disclosure form and the DATMIS system enforces acknowledgement of the Rules of Behavior and the Privacy Act notification each time an authorized user logs on to the DATMIS system. The DOT OST CIO's office ensures that all users, including managers and senior executives participate in system security awareness training before authorizing access to the system. Refresher security training is also done on an annual basis. SAATO employees also complete privacy incident reporting training.

The Department has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of personally identifiable information (PII). These safeguards are designed to achieve the following objectives, ensure the security, integrity, and confidentiality of PII.

These safeguards are designed to achieve the following objectives:

- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII.
- Protect against unauthorized access to or use of PII.

DATMIS is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. Records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in DATMIS is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. Records in the system are protected from

unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

Logical access to the system is guided by the principles of least privilege and need to know. Role- based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs and business functions of the system. Any changes to user roles required approval of the System Manager.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

Employees must complete the privacy courses annually in the official DOT/OST automated electronic learning and training management system. Policies, procedures, and compliance of privacy controls are governed by the OMB, DOT, and OST orders that minimize the use and increase the protection of sensitive material. Driven by role-based profiles, users in DATMIS have segregation of duties and responsibilities that prevent data leakage and minimize the likelihood of inappropriate data utilization.

SAATO ensures that the controls that govern the privacy of DATMIS are tested, reviewed, and assessed at least annually by an independent group of assessors.

Responsible Official

Tonya Templeton
Manager
Substance Abuse Awareness Testing Office, OST-M-14

Approval and Signature

Karyn Gorman
DOT Chief Privacy Officer
Office of Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.07.31 09:31:07 -04'00'