Privacy Impact Assessment
for the

S&T Test Data

DHS Science & Technology Directorate

June 23, 2014

DHS/S&T/PIA-027

Contact Point
Christopher Lee
Privacy Officer
Science & Technology Directorate
(202) 254-0908

Reviewing Official
Karen Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

An integral part of the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) mission is to conduct research, development, testing, and evaluation (RDT&E) on technologies or topics related to improving homeland security and combating terrorism. Some S&T RDT&E activities receive datasets from other DHS components or partner agencies to test, evaluate, and provide feedback on certain research topics, technologies, equipment, and capabilities related to S&T's mission. S&T has published this Privacy Impact Assessment (PIA) to establish baseline protections for test data provided by other DHS components, other government agencies, or other data sharing partners. RDT&E test data that are covered by the PIA are listed in the appendix. The appendix is updated as new projects, programs, systems, or other types of information collection are identified.

Overview

S&T's mission is to improve homeland security by providing state-of-the-art technology to help DHS achieve its goals. S&T accomplishes this mission by using test datasets to research, develop, and evaluate new means of enhancing the performance and utility existing homeland security systems and technologies. Other activities that S&T supports are basic research projects to test or verify hypotheses, theories, or other topics related to homeland security. S&T may collect, use, or share datasets provided by other DHS components or partner agencies for a variety of activities ranging from testing and evaluating technologies to basic research and development projects.

The S&T Privacy Officer analyzes and assesses RDT&E activities based on the information and datasets provided by or shared with partners. The S&T Privacy Officer also evaluates privacy risks associated with the data, and implements privacy mitigation strategies as needed. The DHS Privacy Office uses the Privacy Threshold Assessment (PTA)[1] process to evaluate each project to determine if the project is covered by this PIA, or whether further privacy documentation is required.

Standards[2]

1) The test data may only be used for Research, Development, Test, and Evaluation purposes (RDT&E).
2) S&T does not use the data to make operational decisions.
3) Test data will be destroyed at the end of the pilot, returned to the data owner, or disposed of according to DHS and National Archives and Records Administration

[1] More information on PTAs can be found at http://www.dhs.gov/privacy-compliance.
[2] Established criteria for the S&T Program Managers to follow in order for their projects to qualify for this umbrella PIA, in lieu of having to write a separate PIA.

(NARA) records management schedules.

Retention and Authorities

The respective partner agencies own the datasets, which are subject to the partner agencies' respective systems of records notices and records retention schedule. At the end of the test and evaluation process, the datasets are destroyed or returned to the respective agencies. Projects involving test data sets range from testing new algorithms that better identify fraud, waste, and abuse to testing enhanced homeland security technologies such as fingerprint capture devices. Components will not make operational decisions based on the data results from the test and evaluation process. While a component may implement a new technology or method based on the overall research and testing, it will not use the datasets S&T provides to make an operational decision that could affect an individual based on S&T research.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[3] articulates concepts of 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 Homeland Security Act of 2002[4] states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002[5] and the Homeland Security Act.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system in which the existence is a secret.

The publication of this PIA and attached appendix, as well as other PIAs and SORNs published by the data owners provide notice to individuals that their personal information may be

[3] 5 U.S.C. § 552a (http://www.justice.gov/opcl/privstat.htm).
[4] 6 U.S.C. § 142(2) (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).
[5] 44 U.S.C. § 3501 note (http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm).

used for RDT&E purposes. S&T only collects, maintains, and uses data for RDT&E purposes consistent with the purpose and routine uses of the DHS/S&T – 001 Research, Development, Test and Evaluation Records System of Records Notice (SORN)[6] and respective component SORNs used by data owners for the original data collection. This practice ensures consistency with existing public notice and provides transparency.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual notice for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Test data and reports generated from test data is only used for research and testing. Individuals may be able to opt-out of sharing information or participating in projects, depending on the individual project and methods of information collection used within the project. This option is specific to each project and is handled by the dataset owner on a case by case basis. S&T can remove certain data elements based on direction provided by the data owner.

This PIA along with the DHS/S&T – 001 Research, Development, Test and Evaluation Records SORN serves as notice to individuals for RDT&E information collection and retention by DHS S&T Directorate.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The Homeland Security Act of 2002[7] authorizes S&T to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support RDT&E related to improving the security of the homeland.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

---

[6] DHS/S&T-001 - Research, Development, Test, and Evaluation Records, January 15, 2013, 78 FR 3019.
[7] P.L. No. 107-296, § 302(4) (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).

Test data originates from DHS components and other agencies. Those components and agencies collect the data that is directly relevant and necessary to accomplish the specified purpose, retain the data only as long as necessary to fulfill the specified purpose, and dispose of the data in accordance with their respective records disposition schedules as approved by NARA. At the end of the pilot, the test data is either destroyed or returned to the owner.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Test data is only used for RDT&E purposes. There are some projects that require S&T to share test data with external partners to further its RDT&E objectives. Test data is only shared outside DHS to further RDT&E purposes and with permission from the data owner. Data sharing agreements and memorandums of understanding (MOU) will be used as necessary to limit uses of the test data. External sharing of data is consistent with the Routine Uses listed in the DHS/S&T – 001 Research, Development, Test, and Evaluation Records SORN, and with the Routine Uses of respective component SORNs used by data owners for the original data collection.

S&T determines what data elements are necessary for testing through the DHS Privacy Office privacy compliance life cycle. This process allows S&T to evaluate the necessity of each data element for the testing and ensure that S&T does not collect excess data.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Data quality is managed by the data owners. Test data may come in a variety of formats, including Excel spreadsheets, XML files, paper records, and other formats necessary to provide pertinent information to DHS S&T. The data may be converted to machine-readable formats, but the underlying data will not change. Formatting changes may occur to accommodate machine readability; however, S&T will not make any substantive changes to the underlying test data. S&T informs the data owner if data quality or integrity issues with the test data are identified, and the data owner makes the relevant changes or corrections.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Test data is maintained within secured DHS facilities, using DHS firewalls, stand-alone computers, or secured computer networks. Access to test data is limited to persons with an authorized need-to-know, proper security clearances, and who have also completed annual privacy, information security, and physical security awareness courses. If the data is inaccurate, the data owner will make corrections and provide S&T with a corrected dataset. Individuals may correct data about themselves through the data owner's redress and correction process.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All S&T government personnel and support contractors are required to receive annual privacy awareness, information security, and physical security awareness training. All personnel accessing the test data must have up-to-date privacy and security awareness training credentials, and are also required to abide by federal and DHS privacy and security requirements.

Conclusion

The S&T Test Data PIA establishes privacy requirements governing the use of test datasets provided to S&T by internal DHS entities and external federal agencies. The requirements listed in this PIA protect the privacy of individuals whose records are used in the projects associated with this PIA and allow DHS S&T to fulfill its RDT&E mission goals at the same time.

Responsible Officials

_____

Christopher Lee
Privacy Officer
Department of Homeland Security
Science & Technology Directorate

Approval Signature Page

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix

TSA Pre✓™ Test & Evaluation Program: S&T is working with TSA to Test & Evaluate the Third-Party Prescreening Demonstration associated with the TSA Pre✓™ program. TSA Pre✓™ is a passenger prescreening initiative that identifies low risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints. This project evaluates third-party, private operators to determine if they are capable of developing and implementing processes to prescreen and identify low risk passengers. S&T is testing the algorithms developed by the third-party, private operators. S&T is not testing the DHS/TSA operated and managed portion of the TSA Pre✓™ program. S&T uses government records available to the public to test the algorithms developed by the third-party, private operators. No operational decisions affecting individual passengers will be made based on the testing and evaluation S&T conducts. No PII from third-party, private operators is provided to S&T for test or evaluation. S&T's primary goal is to determine whether or not the third-party, private operator algorithms work. (August 14, 2013).

- DHS/TSA/PIA – 041 TSA Pre✓™ Application Program
- DHS/TSA-021 TSA Pre✓™ Application Program System of Records