Privacy Impact Assessment
for the

Rapid DNA System

DHS/S&T/PIA-024

February 8, 2013

Contact Point
Christopher Miles
Science and Technology Directorate
Department of Homeland Security
(202) 254-6642

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), Science and Technology Directorate (S&T) developed the Rapid Deoxyribonucleic Acid (DNA) System primarily to meet a need to verify family relationships (kinship) in refugee immigration processes. The Rapid DNA System performs rapid, low-cost DNA analysis to meet this need and may also address operational needs of DHS components. S&T is conducting this Privacy Impact Assessment (PIA) because the collection and analysis of DNA information raises potential privacy impacts and concerns.

Introduction

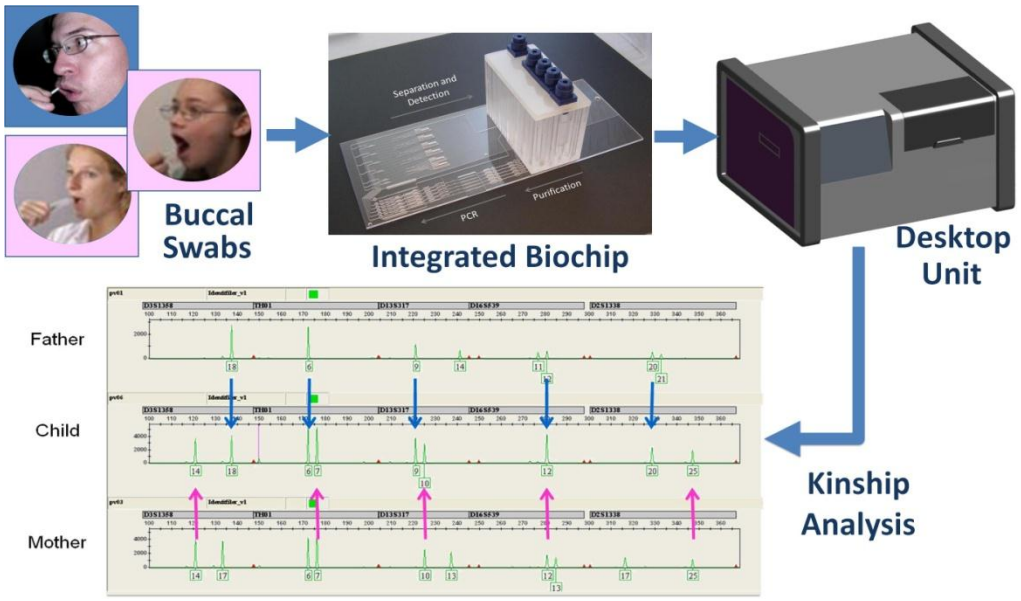
DHS S&T Human Factors and Behavioral Science Division (HFD) developed the Rapid DNA System to address a high-priority technology need for a cost-effective and more efficient way to verify claimed relationships for refugee applicants seeking immigration to the United States. Immigration agencies currently rely on a review of documentary evidence and in-person interviews that are resource-intensive, time-consuming, and susceptible to fraud. In the case that an application is denied for lack of sufficient kinship evidence, the applicant has the option to have his/her DNA processed at his/her own cost by an external certified laboratory and the results provided by the laboratory.

DNA is currently processed in expensive, clean-room laboratories by highly-trained technicians who move the DNA among five or six separate instruments before manually reviewing the results. The laboratory process takes eight to ten hours, in addition to time to transport the sample and results to and from the laboratory. A parent-child DNA laboratory test costs more than $400, with additional child verifications costing $150 each. Maintaining the DNA sample chain-of-custody and avoiding tampering during transport requires that each sample be marked with personally identifiable information (PII) linking the sample to a specific case. The test kits and samples are kept in a secure location (typically in an embassy safe). Transporting, processing, and producing testing results often takes weeks to accomplish.

The Rapid DNA System integrates and automates the current laboratory processes into a single portable instrument that can be used in the field for rapid family relationship verification. The end goal for the Rapid DNA System is to process the DNA in one hour and at a cost of less than $100 per sample. Samples can be collected and processed on site. This greatly reduces chain-of-custody and loss of PII concerns, and provides expedited results.

The Rapid DNA prototype is designed to be portable (the entire unit is roughly the size of a microwave oven) and rugged to withstand shipping to field locations. The system analyzes DNA samples taken from cheek (buccal) swabs. After a cheek swab is taken, it is inserted into a test tube integrated within a disposable microfluidic biochip. The biochip contains all the reagents, buffers, and other fluids and materials necessary to run the DNA analysis. Once the sample is loaded into the biochip, the biochip is then inserted into an automated, integrated desktop unit. The desktop unit contains and provides the power source required to run the reactions and analysis of the DNA sample. The Rapid DNA system processes all DNA data and conducts the analysis.

Each swab has a built-in radio frequency identification (RFID) chip that ensures that the DNA sample cannot be put in the system incorrectly or incorrectly assigned to another person. The chip tracks the cheek swab sample through the entire system processing, from when it is inserted in the biochip to when the resulting DNA profiles are produced, and thus ensures that the results are accurate and for the correct person. Furthermore, once the cheek swab sample is inserted into the biochip, the sample is locked and cannot be removed. Each individual is assigned a subject number, and that number is programmed into the RFID chip when it is processed by the Rapid DNA system so that the names and other PII are not linked to the sample. The RFID is linked only to the subject number; it is not linked to the individual and does not track individual movement.



The Rapid DNA system processes the same short tandem repeat (STR) locations (loci) that are used by the Federal Bureau of Investigation (FBI), INTERPOL, and other accredited DNA laboratories. The loci are chosen specifically because they do not reveal any physical traits, race, ethnicity, disease susceptibility or other sensitive information about an individual. The initial Rapid DNA prototype uses 13 STR loci to verify parent-child relationships. Each loci contains two numbers of two digits each, with the entire DNA profile just 52 characters long (13 loci x 2 numbers x 2 digits per number). A child inherits one half of each loci from each parent. A DNA match is based on a 99.5% or better likelihood that the parent-child relationship is valid. This is the threshold currently set by the American Association of Blood Banks (AABB)-certified laboratories that the U.S. Citizenship and Immigration Services (USCIS) accepts for DNA testing. To allow for verification of grandparent/grandchild and sibling relationships, future prototypes will examine 26 loci. Since grandchildren only receive 1/4 of their DNA from a grandparent, twice as many loci are needed to verify that relationship at the same 99.5% likelihood threshold. These 26 are based on recommendation from the National Institute of Standards and

Technology (NIST)[1] and are also specifically selected from DNA regions that do not reveal any physical traits, race, ethnicity, disease susceptibility, or other sensitive information about an individual.

The performance of the Rapid DNA System prototype is evaluated through laboratory tests by NIST. To accomplish operational validation of the prototype, S&T is working with USCIS to conduct pilot tests in operational settings. The pilot evaluates the system performance under conditions and environments relevant to USCIS officers in the field and assesses the viability of the technology and its potential effectiveness in USCIS operations. This PIA addresses the privacy concerns associated with the new Rapid DNA system.

The Rapid DNA System has access control, encryption, and other privacy-protective measures built in. For example, each Rapid DNA System operator has a unique account to access the system, and is required to sign into the system with a DHS-issued credential and corresponding PIN. System audit and usage logs document individual logins and uses for security purposes, as well as for identification of training and performance issues with the prototype system. The resulting DNA profile data is encrypted within the system. The prototype conducts all of the processing internally and does not have the ability to transmit data electronically. Secure data transmissions in later system iterations may be considered. Such activities would be reported in an updated PIA.

In preparation for the Rapid DNA System, S&T conducted a broad review of DNA needs across DHS operational components and found several consistent needs for verification of family relationships, countering human trafficking, family reunification, identification of victims following mass casualties, and checks against DNA samples of known criminals. Each of these applications require significant policy development or revisions and privacy and civil rights assessments to allow the use of DNA in operational settings.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 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. The Homeland Security Act of 2002, Section 222(2) states that the DHS Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set forth in the Privacy Act of 1974.

Consistent with 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' mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002, and Section 222 of the Homeland

[1] Butler, J.M. and Hill, C.R. (2012) Biology and genetics of new autosomal STR loci useful for forensic DNA analysis. *Forensic Sci. Rev.* 24(1): 15-26.

Security Act of 2002. Given that the Rapid DNA System is a test and evaluation effort that involves the collection of DNA information, rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of the Rapid DNA System as it relates to the FIPPs.

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 the existence of which is a secret.

DHS provides written notice to and obtains informed consent from individuals, when possible, prior to DNA collection and analysis. During the test and evaluation of the Rapid DNA System, S&T only collects and analyzes DNA samples from volunteer participants. For the test and evaluation pilot with USCIS, USCIS will collect DNA samples on a voluntary basis only. All refugee applicants who volunteer to provide DNA receive written and/or verbal notice from USCIS prior to DNA collection notifying them of the use of the DNA. Refugee applicants are not required to provide DNA samples as part of their application.

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 consent 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.

DHS collects DNA samples directly from the individual, typically via a cheek swab. During the test and evaluation of the Rapid DNA System, cheek swabs are taken directly from the volunteers. Similarly, in the USCIS pilot, cheek swabs are taken directly from the family members (i.e., parent and child) claiming family relationships. Refugees voluntarily provide their DNA samples to DHS. DNA testing is not a requirement to complete the refugee application and adjudication process.

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, Pub. L. 107-296, §302(4) authorizes the Science and Technology Directorate 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, S&T is authorized to collect DNA to conduct research and development of the Rapid DNA system and to support USCIS operations. The Rapid DNA System supports USCIS' responsibility to adjudicate refugee applications, as enacted by Congress in the Homeland Security Act of 2002, P.L. 107–296 and 8 CFR Part 207.1, Admission of Refugees.

The Rapid DNA system can only analyze DNA samples and produce a profile that can then be used to verify the family relationship between individuals. The Rapid DNA System is not capable of conducting any other analyses about individuals based on the DNA samples provided. Furthermore, the portion of DNA that is analyzed does not reveal any physical traits, race, ethnicity, disease susceptibility, or other sensitive information about an individual, and will not, under any circumstances, be used for decisions based on those criteria.

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).

The Rapid DNA system requires only a DNA sample to conduct the analysis; no other information, including name, is required for the system. Each sample is assigned a random sample number that is not linked to the individual.

For S&T testing and evaluation purposes, the actual DNA sample is disposed of once the DNA analysis and test results are produced. Test results and DNA analysis may be retained for continued assessment of the technology and compiling a final report on its effectiveness.

Only the DNA test results from the analysis conducted in the AABB accredited laboratory will be taken into account when making the final decision regarding family relationships for refugee status eligibility for those refugee applicants participating in the initial pilot. The results of the Rapid DNA tests will not be used to make final determinations, but will be linked to the individual and maintained in the associated case file.

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.

The Rapid DNA System conducts analysis on the DNA sample only to verify claimed family relationships (initially parent-child and expanded to grandparent-grandchild and siblings in the second phase). The DNA is not used for any other purpose. The DNA will not be used to discriminate in the provision of health or other services and is only used to verify claimed family relationships. Furthermore, the portion of DNA that is analyzed does not reveal any physical traits, race, ethnicity, disease susceptibility, or other sensitive information about an individual.

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.

The Rapid DNA System ensures that each cheek swab sample cannot be put in the system incorrectly or incorrectly assigned to another person. A built in RFID chip in the cheek swab tracks the sample through the entire system processing, from when it is inserted in the biochip to when the resulting DNA profiles are produced, to ensure that the results are accurate and for the correct person. Once the cheek swab is placed into the biochip, it is also locked into place and cannot be removed. This security measure prevents tampering of the sample.

A DNA match is based on a 99.5% or better likelihood that the parent-child relationship is valid. This is the threshold that is currently set by the AABB-certified laboratories that USCIS accepts for DNA testing. It is unlikely that the Rapid DNA system will provide an inaccurate DNA match. If USCIS receives an inconclusive test result, it may re-collect and rerun the sample through the system. Participants, at their own expense, can also submit their DNA samples to an AABB-certified laboratory for independent testing.

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.

System access requires a DHS-issued identification card, along with the corresponding PIN. Once the cheek swab sample is taken and inserted into the biochip, the cheek swab sample locks in place and cannot be tampered with or removed. The resulting DNA profile data is encrypted within the system to prevent unauthorized access to the DNA profile and analysis. The prototype system does not have Internet connectivity and cannot transmit information electronically or wirelessly. Secure transmissions in future iterations may be evaluated as needs requirements are identified and as permitted by security and privacy policies.

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.

Each Rapid DNA system operator has a unique account to access the system, and is required to sign into the system with his or her DHS-issued credentials and PIN. Use of the system is also logged and a secure digital trail of user actions is maintained, not only for security purposes but for identification of training and performance issues with the prototype system. Each operator receives training on how to explain the Rapid DNA system to immigration applicants, collection of consent forms, protection of PII, and proper methods for swab collection and system operation.

A DNA match is based on a 99.5% or better likelihood that the parent-child relationship is valid. This is the threshold that is currently set by the AABB-certified laboratories that USCIS accepts for DNA testing. It is unlikely that the Rapid DNA system will provide an inaccurate DNA match. Any inconclusive test results would be due to a physical obstruction of the system (i.e., an air bubble or debris in the biochip preventing the reagents or fluids from flowing through the system to run the required

reactions). If USCIS receives an inconclusive test result, it may re-collect and rerun the sample through the system. Participants, at their own expense, can also submit their DNA samples to an AABB-certified laboratory for independent testing.

Conclusion

The Rapid DNA System integrates and automates current laboratory DNA processes to create a capability for rapid and cost-effective DNA testing. The methodology and techniques mimic what is currently being done by the FBI and other accredited laboratories; the Rapid DNA System simply miniaturizes the process, making it portable and accessible for DHS operational users. The system is not linked to any other DHS database and is not connected to the DHS network. In the USCIS test and evaluation pilot, the technology analyzes DNA samples provided by individuals, and verifies claimed familial relationships. Privacy-protective measures have been built into the system to minimize inaccuracies and to prevent unauthorized access. The portion of DNA that is analyzed by the system does not reveal any physical traits, race, ethnicity, disease susceptibility, or other sensitive information about an individual, and will not be used for purposes other than verifying claimed familial relationships. Furthermore, DHS operational components have the responsibility to ensure that standard operating procedures and policies are in place to guide the collection, use, and retention of the DNA analysis and information prior to deployment.

Responsible Officials

Christopher Miles
Program Manager
S&T Human Factors and Behavioral Science Division

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security