9110-9F

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0025]

Privacy Act of 1974**;** Science & Technology Directorate-001 Research, Development, Test, and Evaluation Records System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/Science and Technology Directorate-001 Research, Development, Test, and Evaluation System of Records." This system of records allows the Department of Homeland Security/Science and Technology Directorate to collect and maintain records collected in support of, or during the conduct of, Science & Technology-funded research, development, test, and evaluation activities. As a result of the biennial review of this system, routine uses have been updated. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0025 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change and may be read at http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Christopher Lee, STPrivacy@hq.dhs.gov, the Science & Technology Directorate's Privacy Office, Mail Stop: 0205, Department of Homeland Security, 245 Murray Lane, SW, Washington, D.C. 20528. For privacy issues, please contact: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) proposes to

update and reissue a current DHS system of records titled, "DHS/S&T-001 Research, Development, Test, and Evaluation System of Records."

An integral part of the Department of Homeland Security (DHS) Science & Technology Directorate's (S&T) mission is to conduct research, development, testing, and evaluation (RDT&E activities) on topics and technologies related to improving homeland security and combating terrorism. Some RDT&E activities involve the collection of personally identifiable information. This system of records notice covers records collected in support of, or during the conduct of, DHS/S&T-funded RDT&E activities, when those records are retrieved by personal identifier.

As a general rule, the information collected will be used by DHS/S&T solely for the purposes of supporting RDT&E activities (e.g., testing and evaluating a screening technology or obtaining feedback on a technology from volunteer participants). S&T will not use the information collected for law enforcement, intelligence, or any purpose other than RDT&E. This system of records notice only covers the collection and use of information for the purpose of RDT&E activities. In situations when DHS/S&T-funded RDT&E activities directly involve law enforcement, intelligence personnel, and/or other operational entities, a separate SORN is required to address any activities from which information collected would be used in operations, to support operational decisions, or any purpose other than RDT&E activities. An exception to the above general rule limiting the use of collected information to RTD&E activities is if, during a human subject testing activity, the individual provides information that indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations. Only in that limited situation, the information collected may be referred to federal, state, tribal,

local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, pursuant to Routine Use G, below.

The Routine Uses have been updated to include Routine Use "H," disclosure to the news media and the public. Additionally, this notice includes non-substantive changes to simplify and clarify the formatting and text of the previously published notice. The updates do not have a significant impact on individual privacy. All current privacy protections and considerations remain intact ensuring individual privacy is protected during S&T RDT&E activities, including conducting a Privacy Impact Assessment (PIA) and using technical safeguards and access controls to protect data from unauthorized use. The updates specify that any law enforcement, intelligence personnel, or operational partners collaborating with S&T may make operational decisions based on information collected during S&T RDT&E activities, if they have appropriate legal authority and an appropriate SORN is in place.

This updated system will be included in DHS' inventory of record systems.

II. The Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which federal government agencies collect, maintain, use and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other particular assigned to an individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and

legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is a description of the DHS/S&T-001 Research, Development, Test, and Evaluation Records System of records.

In accordance with 5 U.S.C. 552a(r), a report on this system has been sent to Congress and to the Office of Management and Budget.

System of Records:

Department of Homeland Security/S&T-001

System name:

DHS/S&T-001 Research, Development, Test, and Evaluation Records

Security Classification:

Unclassified

System location:

Records are maintained at the S&T Headquarters in Washington, D.C., in S&T field offices, and at public or private institutions, including the National Labs, conducting research funded by S&T.

Categories of individuals covered by the system:

Categories of individuals covered by this notice include voluntary participants in S&T-funded research (note: all S&T-funded research that involves human subjects research is conducted in accordance with 45 CFR part 46 and is reviewed by a certified Institutional Review Board); individuals whose names may appear in publicly available documents (e.g., newspapers and academic articles) about terrorism, terrorist events,

violent groups, or other topics related to terrorism research; individuals whose personally identifiable information may be collected through DHS operations and maintained by other DHS components; individuals whose images, biometrics, physiological features, or other information may be intentionally (with notice to and consent by the individual) or incidentally captured during testing of S&T technologies; subject matter experts who publish articles related to terrorism or biomedical and life sciences research; and subject matter experts who voluntarily consent to be included in a database of experts.

Categories of records in the system:

S&T RDT&E Records will vary according to the specific project. The information may include, but is not limited to, an individual's:

- Name;
- Age;
- Gender;
- Contact information;
- Birthplace;
- Ethnicity;
- Level of education;
- Occupation;
- Institutional or organizational affiliation;
- Publication record, such as article and publication titles, dates and sources;
- Medical history;
- Lifestyle information (e.g., caffeine or tobacco use);
- Publicly available reports of criminal history;

- Video or still images;
- Other images (e.g., infrared thermography, terahertz, millimeter wave);
- Audio recordings;
- Fingerprints, iris images, DNA or other biometric information; and
- Physiological measurements collected using sensors (e.g., heart rate, breathing pattern, and electrodermal activity).

Authority for maintenance of the system:

The Homeland Security Act of 2002, Pub. L. No. 1007-296, § 302(4) (codified at 6 U.S.C. § 182(b)), 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 under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support research and development related to improving the security of the homeland. When research includes human subjects, S&T complies with the provisions of DHS Management Directive 026-04, "Protection of Human Subjects", which adopts the regulations set forth in 45 CFR part 46 and establishes Departmental policy for the protection of human subjects in research.

Purpose(s):

Records are collected for the purpose of furthering S&T's mission to push innovation and development, and the use of high technology in support of homeland security. The purposes of the records are to:

- Understand the motivations and behaviors of terrorists, individuals that engage in violent or criminal activities, terrorist groups, and groups that engage in violent or criminal activities.
- Understand terrorist incidents and the phenomenon of terrorism and identify trends and patterns in terrorist activities.
- Collect and maintain searchable records of individuals (such as subject matter experts on chemical weapons) and/or their characteristics and professional accomplishments, organized according to categories useful for the purpose of collaboration or conduct of research, including research to determine the efficacy and utility of new or enhanced technologies intended for eventual transition to and use by S&T's customers.
- Evaluate the performance and utility to the future customer of an experimental homeland security or first responder technology or product in a laboratory or "real-world" setting.
- Test the accuracy of a research hypothesis. (For example, S&T might hypothesize that an individual's behavior changes in a detectable manner when he or she is being deceitful, and then design a research experiment to test that hypothesis.)
- Answer a research question. (For example, "Can an experimental screening technology distinguish between threat objects and non-threat objects?").
- Conduct testing and evaluation of an experimental technology at the request of or on behalf of a customer.
- Conduct research and development to solve a technical problem for a customer.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3):

A. To the Department of Justice (DOJ), including U.S. Attorney Offices, or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. any employee of former employee of DHS in his/her official capacity;

3. any employee or former employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. the United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or

oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a

violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

RDT&E records maintained in hard copy are stored in a locked file cabinet or safe. Electronic records are stored in computer files that require a password for access and are protected by a firewall. Data and systems are encrypted as necessary, pursuant to DHS guidelines.

Retrievability:

In most cases, S&T RDT&E is focused on evaluating the performance of a given experimental technology or system. Thus, only the aggregated performance data (e.g., the technology has a 5% false positive rate, or the technology is accurate 92% of the time) is

important and relevant to S&T. For this reason, S&T RDT&E records are not as a matter of course retrieved by name or other identifier assigned to the individual. However, S&T may need to access RDT&E records by name or other identifier in order to make corrections to an individual's record, resolve an anomaly related to a specific individual's record, and/or link disparate pieces of information related to an individual. For example, if an individual informed a researcher that he or she had inadvertently provided incorrect information regarding his or her medical history, the researcher would retrieve that individual's record using the research identifier in order to correct the erroneous data.

Safeguards:

All RDT&E records are protected by employing a multi-layer security approach to prevent unauthorized access to sensitive or personal data through appropriate administrative, physical, and technical safeguards. Protective strategies such as implementing physical access controls at DHS facilities; ensuring confidentiality of communications using tools such as encryption, authentication of sending parties, and compartmentalizing databases; and employing auditing software and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

S&T RDT&E records are also monitored for changes to the source data. The program manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data transactions for the purpose of conducting privacy or security incident investigations. S&T RDT&E records are secured in full compliance with the requirements of DHS IT

Security Program Handbook. This handbook establishes a comprehensive information security program.

Retention and disposal:

All records will be maintained in accordance with the NARA-approved retention schedule. All existing S&T RDT&E records fall under General Records System 20, which covers the disposition of electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records. According to General Records System 20, records should be "delete[d]/destroy[ed] when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes." Electronic records will be deleted from all computers, storage devices, and networks, and paper records will be shredded. Oftentimes, PII collected during the project is retained for the duration of the project; at the conclusion of the project, PII is destroyed. However, researchers may retain aggregated research data (without PII) indefinitely, as it may help inform future RDT&E efforts.

System manager(s) and address:

S&T Privacy Office, Mail Stop: 0205, Department of Homeland Security, 245 Murray Lane, SW, Washington, D.C. 20528.

Notification procedure:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to S&T FOIA Officer, Mail Stop: 0205 Department of Homeland Security, 245 Murray Lane,

SW, Washington, D.C. 20528, specific FOIA contact information can be found at http://www.dhs.gov/foia under "contacts."

When seeking records about yourself from this system of records or any other S&T system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. 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. While no specific form is required, you may obtain forms for this purpose from Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and

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.

Without the above information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See “Notification procedure” above.

Contesting record procedures:

See “Notification procedure” above.

Record source categories:

S&T RDT&E records include (1) records collected directly from the individual; (2) publicly available documents (e.g., articles from newspapers and academic journals); (3) records collected from the individual using sensors (e.g., a heart rate monitor) or technologies (e.g., cameras, audio recorders, infrared thermography or other images, or biometric devices).

Exemptions claimed for the system:

None.

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-00602 Filed 01/14/2013 at 8:45 am; Publication Date: 01/15/2013]