9110-9F

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2021-0038]

Privacy Act of 1974; System of Records

AGENCY: Science & Technology Directorate, U.S. Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/Science & Technology Directorate (S&T)-001 Research, Development, Test, and Evaluation System of Records." This system of records allows DHS/S&T to collect and maintain records in support of, or during the conduct of, S&T-funded research, development, test, and evaluation activities. Information is 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. This modified system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system of records will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2021-0038 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: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2021-0038. All comments received will be posted without change to 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: Maria Petrakis, (202) 254-7748, STPrivacy@hq.dhs.gov, S&T Privacy Officer, Science & Technology Directorate, Mail Stop: 0205, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20528. For privacy questions, please contact: Lynn Parker Dupree, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) Science & Technology Directorate (S&T) proposes to modify and reissue a current DHS system of records titled, "DHS/S&T-001 Research, Development, Test, and Evaluation System of Records." S&T's mission is to conduct research, development, testing, and evaluation (RDT&E or 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 covers records collected in support of, or during the conduct of, DHS/S&T-funded RDT&E activities in support of DHS Components and other partners in the Homeland Security Enterprise. Records can be collected through RDT&E activities such as testing and evaluating a screening technology, obtaining feedback on a technology from

volunteer participants, or evaluating analytic tools using publicly available information.

Pursuant to its statutory mandate, S&T engages in both basic and applied RDT&E. Basic research is that RDT&E which is normally conducted without specific applications toward processes or products in mind. For example, S&T researchers often engage in the development of knowledge products (e.g., white papers, literature reviews, peer-reviewed scholarly articles) for distribution to the Homeland Security Enterprise at large. This type of RDT&E is not in response to an external demand signal; rather, individual subject matter experts (SME) use their expertise and experience to advance the science of their respective fields. Because these knowledge products are shared with external entities, S&T refers to these external entities as S&T's "customers." Applied research is that RDT&E which is conducted to determine the means by which a recognized and specific operational need may be met. For example, if the Transportation Security Administration (TSA) identifies the need for a novel methodology of screening carry-on luggage at airport checkpoints, TSA would task S&T to develop this novel methodology through RDT&E activity. In instances where the RDT&E demand signal originates from outside of S&T, the originator is also referred to as an S&T's "customer."

In situations where DHS/S&T-funded RDT&E activities directly involve law enforcement, intelligence personnel, and/or other operational entities, a source-system system of records notice (SORN) is relied upon to cover any records collected that are to be used in operations, to support operational decisions, or any purpose other than RDT&E activities. However, there could be situations, for example, during a human subject testing activity, whereby an individual provides information that indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, for which such records would be covered by this SORN, and subsequently may be disclosed to external third parties that are charged with investigating or

prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, described in Routine Use G below.

DHS/S&T is updating this system of records notice for several reasons, to include the maintenance of classified records, correct the citation of the authority which outlines the responsibilities of the Under Secretary for Science & Technology, add additional categories of individuals and categories of records, and modify Routine Uses. Individuals covered by this system of records now include individuals whose names or other identifying information may appear on social media platforms used or accessed by S&T for RDT&E purposes related to public safety, terrorism (including terrorist and targeted violence events), violent or criminal groups, or other topics related to preventing terrorism; counterterrorism; chemical, biological, and related weapons and materials; biomedical and life sciences research; or other homeland security information of interest to DHS/S&T in the performance of RDT&E activities. Additional records added to this system include Social Security number (SSN); social media handle, online user name, or other online identifier; research or other unique identifier; Uniform/Universal Resource Locator (URL); Internet Protocol (IP) address; Media Access Control Address (MAC); and Computer name to account for information collected and maintained related to social media, other publicly available information, and other RDT&E activities. S&T is also updating this SORN to clarify the types of biometric samples and data that may be collected.

DHS/S&T is also updating this SORN to include additional record source categories to include information obtained from publicly available sources, such as social media and the Internet; other governmental agencies and entities; critical infrastructure owners and operators; other private sector entities and organizations; and free or fee-based commercial data providers. This SORN also addresses new policies and practices regarding storage, retrieval, retention, and disposal of records.

Further, DHS/S&T is modifying Routine Use "E" and adding Routine Use "F" to conform to the breach requirements in OMB Memorandum M-17-12. The previous Routine Use "F" has been re-lettered as Routine Use "H," the content of the previous Routine Use "G" has been modified to conform with current DHS requirements, and Routine Use "I" has been added to account for sharing to appropriate governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology. Subsequent Routine Uses have been renumbered to account for these changes.

Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in DHS/S&T-001 Research, Development, Test, and Evaluation System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/S&T may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

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

II. Privacy Act

The fair information practice principles found in the Privacy Act underpin the 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 identifying

particular assigned to the individual. In the Privacy Act, an individual is defined as U.S. citizens and lawful permanent residents. Similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/S&T-001 Research, Development, Test, and Evaluation System of Records. In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS)/Science & Technology Directorate (S&T)-001 Research, Development, Test, and Evaluation (RDT&E) System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at the S&T Directorate Headquarters in Washington, D.C., and field offices, and at public or private institutions conducting S&T-funded RDT&E activities.

SYSTEM MANAGER(S): Under Secretary for Science and Technology, Mail Stop: 0205, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20528; (202) 254-7748; STPrivacy@hq.dhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Homeland Security Act of 2002, Public Law 107-296, Sec. 302 (codified at 6 U.S.C. sec. 182) authorizes the 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 research and development related to improving the security of the homeland. To the extent an activity meets the definition of research involving human subjects, DHS complies with the regulations set forth in 6 CFR part 46..

PURPOSE(S) OF THE SYSTEM: Records are collected for the purposes of furthering S&T's mission to push innovation and development and use technology in support of homeland security. The purposes of this system 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 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 or to provide scientific and technical expertise in support of emergency preparedness and response;
- Evaluate the performance and utility to the future customer of an experimental homeland security 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; and
- Conduct research and development to solve a technical problem for a customer.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals include voluntary participants in S&T-funded RDT&E activities such as field exercises or assessments, voluntary participants in human subjects research (note: all S&T-funded human subjects research is conducted in accordance with 45 CFR 46 and is reviewed by a certified Institutional Review Board); individuals whose names or other identifying information may appear in publicly available documents (e.g., newspapers, academic articles, and websites) or on social media platforms about public safety, terrorism (including terrorist and targeted violence events), counterterrorism, violent or criminal groups, or other topics related to chemical, biological, and related weapons and materials, biomedical and life sciences research, or other homeland security information of interest to DHS/S&T in the performance of RDT&E activities. This system of records also covers 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, counterterrorism, chemical, biological, 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's RDT&E activities will vary according to the specific project. The information may include an individual's:

- Name;
- SSN;
- User name;
- Online identifier (e.g., social media handle);

- Research or other unique identifier;
- Uniform Resource Locator (URL);
- Internet Protocol (IP) address;
- Media Access Control (MAC) Address;
- Computer name;
- Age;
- Gender;
- Contact information;
- Birthplace;
- Ethnicity;
- Level of education;
- Occupation;
- Institutional or organizational affiliation;
- Publication record (e.g., article and publication titles, dates and sources);
- Medical history and other health-related information;
- Lifestyle information (e.g., caffeine use, tobacco use);
- Publicly available reports of criminal history or violence;
- Video or still images;
- Other images (e.g., infrared thermography, terahertz, millimeter wave);
- Audio recordings;
- Biometric samples (e.g., facial images, speech/voice, fingerprints, deoxyribonucleic acid (DNA), iris, human tissue, or other biometric information);
- Biometric data (e.g., Fingerprint Identification Number, voice and contactless fingerprints, biometric templates, typing cadence, cardiac signature, vascular patterns); and

- Physiological measurements collected using sensors (e.g., heart rate, breathing pattern, electrodermal activity).

RECORD SOURCE CATEGORIES: Records are obtained from (1) individuals directly; (2) publicly available information (e.g., social media platforms, news media outlets, Internet search engines, academic and scientific publications); (3) sensors (e.g., records collected from the individual using sensors, such as a heart rate monitor) or technologies (e.g., cameras, audio recorders, infrared thermography or other images, biometric devices); (4) federal, state, local, territorial, tribal governments and agencies; (5) other domestic agencies; (6) foreign governments and agencies; (7) multinational or nongovernmental organizations; (8) critical infrastructure owners and operators; (9) private sector entities and organizations; and (10) free or fee-based commercial data providers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 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. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or 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 or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when 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. secs. 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

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, when 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 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.

I. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology.

J. 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, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/S&T stores records in this system electronically or on paper in secure facilities, typically, in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: S&T may retrieve records by any of the information listed in the Categories of Records above.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: All records are maintained in accordance with the appropriate NARA-approved retention schedules. Different NARA-approved records retention schedules apply to specific RDT&E records, depending on the RDT&E activity. For example, Technical Information Bulletins, Technical Notes, Test and Evaluation Case Files, Test and Evaluation Files, Test and Evaluation Product Packages, Test Procedures and Protocols, and Test Team Assessment Letters fall under DHS Schedule 109-026-003, Scientific and Technological Research and Innovation. DHS/S&T must review Technical Information Bulletins and Technical Notes annually in accordance with N1-563-08-30 and delete or destroy records that have been inactive for five years. Test and Evaluation Case Files and supporting documentation is scheduled to be destroyed at the end of the calendar year five years after the completion of the test, exclusive of Test and Evaluation Final Reports, which are scheduled to be destroyed five years after the tested device, system, or equipment is removed from operation in accordance with N1-563-08-13-7. Test and Evaluation File records, excluding Final Reports, are scheduled to be destroyed at the end of the calendar year five years after completion or cancellation of a project or one year after the responsible office determines the record is no longer needed for legal, audit, administrative or business purposes. Final Reports must be reviewed annually and destroyed or deleted after five years of inactivity, in accordance with N1-563-09-4-4. DHS/S&T destroys Test and Evaluation Product Packages 10 years after the testing and evaluation is completed as required by N1-563-08-13-8.

DHS/S&T retains other RDT&E records on specific topics, issues, or projects in accordance with DHS Schedule 401-000-001a, Subject Files. The Subject Files are permanent and transferred to the National Archives after 10 years, in accordance with N1-563-07-13-11. DHS/S&T retains records involving inventions or patents according to DHS Schedule 105-012-002, Intellectual Property Protection, and N1-563-07-17-9. For

trademarks, DHS/S&T destroys the records at the end of the calendar year, 20 years after the date of issuance. For patents, DHS/S&T destroys the records at the end of the calendar year, 40 years after the date of issuance. For copyright, DHS/S&T destroys the records at the end of the calendar year, 150 years after the date of issuance. For trade secrets, DHS/S&T destroys the records at the end of the calendar year, 20 years after the date when developed/discovered or when the trade secret is no longer valuable, whichever is later. Research and Development-related memoranda of understanding or agreement fall within DHS Schedule 105-012-003, Intellectual Property Protection, and are destroyed or deleted three years from when the agreement is terminated under N1-563-09-11-1. Program Evaluation records including Technical Assessments and Legal and Regulatory Compliance Records fall within DHS Schedule 301-092-002, Program Evaluation, and N1-563-08-30-5. DHS/S&T is required to destroy or delete Technical Assessment project files, excluding Final Reports, at end of the calendar year five years after completion or cancelation of assessment or one year after the responsible office determines the records are no longer needed for legal, audit, administrative, or business purposes. DHS/S&T must destroy Program Evaluation legal and regulatory compliance records when the records are five years old.

Given the scope of RDT&E activities, additional NARA-approved schedules apply to S&T records. Some records are permanent records and other records are temporary records. The records have different disposition instructions based on the applicable records retention schedule.

DHS/S&T also has RDT&E records schedule requests pending, for example, for DHS/S&T National Laboratory research and development files, not used in law enforcement cases, and records that document compliance with standards-organization requirements to carry out test and calibration. Records subject to pending records

schedule requests shall be retained until a records retention schedule has been approved by NARA.

Researchers may retain aggregated research data indefinitely, as it may help inform future RDT&E efforts.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/S&T safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. S&T has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system 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 or permissions.

RECORD ACCESS PROCEDURES: Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Component Privacy Officer or Component Freedom of Information Act Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655, or electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about him or her may be available under the Freedom of Information Act. When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name,

current address, and date and place of birth. The individual must sign the request, and the individual's 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. An individual may obtain more information about this process at http://www.dhs.gov/foia. In addition, the individual should, whenever possible:

- Describe the records sought, including any circumstances or reasons why the Department would have information being requested;
- Identify which component(s) of the Department or Department Headquarters Office he or she believes may have the information;
- Specify the timeline when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Headquarters Office or component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include a statement from the living individual verifying the identity of the individual, as described in the verification steps above, and provide a statement from the living individual certifying the individual's agreement that records concerning the individual may be released to you.

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

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the

amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, individuals may seek to amend records following the "Record Access Procedures" above. DHS/S&T, in its discretion, may choose to make the requested amendment. However, neither this system of records notice, nor DHS/S&T's making a requested amendment, confers to individuals any right to access, contest, or amend records not covered by the Privacy Act or Judicial Redress Act.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None. When this system receives a record from another system exempted in that source system under 5 U.S.C. sec. 552a, DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated.

HISTORY: 78 Fed. Reg. 3019 (January 15, 2013).

****

Lynn Parker Dupree,
Chief Privacy Officer,
U.S. Department of Homeland Security.
[FR Doc. 2021-22849 Filed: 10/19/2021 8:45 am; Publication Date: 10/20/2021]