9112-FP

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0026]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "Department of Homeland Security/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System of Records." This system of records describes DHS's collection, use, and maintenance of records on individuals associated with DHS and its facilities during a declared public health emergency. This newly established 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 new system 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-2020-0026 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: Constantina Kozanas, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0026. 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 and privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The Secretary of the Department of Health and Human Services (HHS) may, under section 319 of the Public Health Service (PHS) Act (codified at 42 U.S.C. sec. 247d), declare that: a) a disease or disorder presents a public health emergency; or b) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists. The declaration lasts for the duration of the emergency or 90 days, but may be extended by the Secretary. Congress must be notified of the declaration within 48 hours. The Department of Homeland Security must ensure the safety of its workforce, including when the Secretary of HHS or the responsible, designated State official declares and determines that a public health emergency exists.

Responses to public health emergencies depend on the nature of the emergency, but in the context of infectious disease or other events that can cause and spread deleterious health impacts to DHS personnel and others in DHS facilities, in order to ensure a safe and secure workspace, DHS may collect information on DHS personnel (meaning employees, detailees, interns, and volunteers), contractors, long-term trainees, and visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS.

This system of records will cover information collected on DHS personnel, contractors, long-term trainees, and visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS who have contracted or may have been exposed to a suspected or confirmed disease or illness that is the subject of a declared public health emergency. The information collected may include identifying and contact information of individuals who have been suspected or confirmed to have contracted a disease or illness, or who have been exposed to an individual who had been suspected or confirmed to have contracted a disease or illness, related to a declared public health emergency; individual circumstances and dates of suspected exposure; and health status information. DHS maintains this information to reduce the spread of the disease or illness among DHS personnel, contractors, long-term trainees, and visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS. In certain instances, depending on the type of record collected and maintained, for federal employees, this information will also be maintained and covered by Office of Personnel Management/Government-10 Employee Medical File System Records (75 FR 35099, June 21, 2010). However, any collection and use of records covered by the DHS/ALL-

047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System of Records is only permitted during times of a declared public health emergency and when the circumstances permit the Department to collect and maintain such information on the various categories of DHS personnel, contractors, long-term trainees, and visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS.

It must first be determined that the circumstances surrounding the declared public health emergency permit the Department to collect and maintain the information that may fall within the scope of this system of records. To make this determination, these circumstances must be examined in conjunction with all applicable laws, including the U.S. Constitution, federal privacy laws, federal labor and employment laws, and federal workforce health and safety laws. Different laws may apply depending upon the type of information at issue, who the information pertains to, who collected the information, and how the information is collected, maintained, and used by the Department.

For instance, when collecting information on DHS employees, there are several employment laws that govern the collection, dissemination, and retention of employee medical information. These employment laws include the Americans with Disability Act (ADA), the Rehabilitation Act of 1973 (Rehab Act), and the Occupational Safety and Health Act of 1970 (OSH Act). Generally, under federal employment laws, medical information pertaining to employees is confidential and may be obtained by an employer only for certain reasons and only at certain points in the employment relationship. During a public health emergency, an employer may be permitted to collect certain employee medical information that it would not otherwise be permitted to collect depending upon

the circumstances. Whether an employer is permitted to collect otherwise confidential employee medical information during a public health emergency depends upon whether an employee or a potential employee poses a "direct threat" to others within the meaning of the Americans with Disabilities Act of 1990, the Americans with Disabilities Amendments Act of 2008, and the Rehabilitation Act of 1973. Again, this system of records will apply if it is determined that the circumstances permit the Department to legally collect the employee medical information at issue in the first instance.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System of Records may be shared with other DHS Components that have a need to know the information to carry out their mission essential functions, but only if it is first determined that the information may be shared under all other applicable laws and DHS policies.

In addition, to the extent permitted by law, DHS 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 newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice 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 identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right 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/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency 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: Department of Homeland Security (DHS)/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System of Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at the DHS Headquarters and Component offices in Washington, D.C. and field offices, and contractor-owned and operated facilities.

SYSTEM MANAGER(S): Chief, Medical Quality & Risk Reduction Branch, Workforce Health and Safety, Office of the Chief Human Capital Officer, Department of Homeland Security, OCHCOPrivacyOfficer@hq.dhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Section 319 of the Public Health Service (PHS) Act (42 U.S.C. sec. 274d); DHS Chief Medical Officer's authorities pursuant to 6 U.S.C. sec. 350 and 6 U.S.C. sec. 597; 6 U.S.C. sec. 464; 21 U.S.C. sec. 360bbb-3; 40 U.S.C. sec. 1315; American with Disabilities Act, including 42 U.S.C. sec. 12112(d)(3)(B), 29 CFR 602.14, 1630.2(r), 1630.14(b)(1), (c)(1), (d)(4); Medical Examinations for Fitness for Duty Requirements, including 5 CFR Part 339; Workforce safety federal requirements, including the Occupational Safety and Health Act of 1970, Executive Order 12196, 5 U.S.C. sec. 7902; 29 U.S.C. Chapter 15 (e.g., 29 U.S.C. sec. 668), 29 CFR Part 1904, 29 CFR 1910.1020, and 29 CFR 1960.66; and United States Coast Guard authorities, including 10 U.S.C. Subtitle A, Part II, Chapter 55, Medical and Dental Care, as applicable, 14 U.S.C. sec. 504(a)(17), 14 U.S.C. sec. 936, 14 U.S.C. sec. 3705, 42 U.S.C. sec. 253, 32 CFR Part 199, and 42 CFR 31.2 - 31.10.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain records to protect the Department's workforce and respond to a declared public health emergency. For instance, DHS may use the information collected to conduct contact tracing.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Department personnel (including employees, detailees, interns, and volunteers), long-term trainees (such as Federal Law Enforcement Training Centers (FLETC) students), contractors, and visitors (all other federal employees, applicants, and members of the public) at or on buildings, grounds, and properties that are owned, leased, or used by DHS who are suspected or confirmed to have a disease or illness that is the subject of a declared public health emergency, or may have been or could have been exposed to someone who is

suspected or confirmed to have a disease or illness that is the subject of a declared public health emergency.

CATEGORIES OF RECORDS IN THE SYSTEM:

For DHS personnel, long-term trainees, and contractors, the following information may be collected:

- Individual's full name;
- Preferred phone number(s);
- DHS duty location, facility, and specific work space accessed;
- Preferred email address(es);
- Individual's supervisors' name, address, and contact information, and/or the contractor's supervisor/contracting officer representative name, address, and contact information;
- Date(s) and circumstances of the individual's suspected or actual exposure to disease or illness including symptoms, as well as locations within DHS workplace where an individual may have contracted or been exposed to the disease or illness; and names and contact information of other employees, long-term trainees, contractors, or visitors that the individual interacted with at or on a DHS workspace, facility, or grounds during time the individual was suspected to or had contracted the disease or illness;
- Current work status of the individual (e.g., administrative leave, sick leave, teleworking, in the office) and affiliated leave status information;
- Other individual information directly related to the disease or illness (e.g., testing results, symptoms, treatments, source of exposure).

For visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS, the following information may be collected:

- Full name;
- Preferred phone number(s);
- Preferred email address(es);
- Date(s) and time(s) of entrance and exit from DHS workspaces, facilities, and grounds;
- Name(s) of all individuals encountered while in or at DHS workspaces, facilities, and grounds.
- Information indicating plans on entering a DHS workspace, facility, or grounds in the near future; and
- Other records covered by DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records (75 FR 5609, February 3, 2010) that are relevant and necessary to achieve the purpose of this SORN.

RECORD SOURCE CATEGORIES: When permitted by applicable law, records may be obtained from DHS personnel, long-term trainees, contractors, and visitors at or on buildings, grounds, and properties that are owned, leased, or used by DHS; their family members; federal, state, local, tribal, territorial, and foreign government agencies; employers and other entities and individuals who may provide relevant information on a suspected or confirmed disease or illness that is the subject of a declared public health emergency.

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 agency 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. sec. 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 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.

H. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, to the extent permitted by law, and in consultation with DHS legal counsel, for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to

combat other significant public health threats; appropriate notice will be provided of any identified health risk.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media. Medical information collected is maintained on separate forms and in separate medical files and are treated as a confidential medical record.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS may retrieve records by any of the categories of records, including name, location, date of exposure, or work status.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: DHS is in the process of developing a records schedule for declared public health emergency records. However, to the extent applicable, to ensure compliance with Americans with Disabilities Act (ADA) and the Rehabilitation Act, medical information must be "maintained on separate forms and in separate medical files and be treated as a confidential medical record." 42 U.S.C. sec. 12112(d)(3)(B); 29 CFR 1630.14(b)(1), (c)(1), (d)(4)(i). This means that medical information and documents must be stored separately from other personnel records. As such, the Department must keep medical records for at least one year from creation date. 29 CFR 1602.14. Further, any records compiled under this SORN and incorporated into an occupational individual medical case record pursuant to the OSH Act must be maintained in accordance with 5 CFR Part 293.511(b) and 29 CFR 1910.1020(d), and must be destroyed 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer,

in accordance with NARA General Records Schedule (GRS) 2.7, Item 60, and NARA records retention schedule DAA-GRS-2017-0010-0009, to the extent applicable. Visitor processing records are covered by GRS 5.6, Items 110 and 111, and must be destroyed when either two or five years old, depending on security level, but may be retained longer if required for business use, pursuant to DAA-GRS-2017-0006-0014 and -0015.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS 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 Chief Privacy Officer or the appropriate Headquarters or component's FOIA Officer whose contact information can be found at http://www.dhs.gov/foia under "Contact 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, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you 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. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes 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;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

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 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.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Constantina Kozanas,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2020-16466 Filed: 7/29/2020 8:45 am; Publication Date: 7/30/2020]