9110-9B

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2017-0019]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to modify and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records." This system of records allows the Department of Homeland Security to collect and maintain records on the results of law enforcement activities in support of the protection of property owned, occupied, or secured by the Department of Homeland Security and its Components, including the Federal Protective Service, and individuals maintaining a presence or access to such property. The Department of Homeland Security is updating this system of records notice to, among other things, (1) modify the category of individuals, (2) modify the category of records, (3) modify two existing routine uses, and (4) add a new routine use. The Department of Homeland Security is also issuing a Notice of Proposed Rulemaking to add a new exemption from certain provisions of the Privacy Act, elsewhere in the Federal Register. This new exemption is needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the additional exemptions are required to preclude subjects of these activities from frustrating

ongoing operations; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS's ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension. The existing Privacy Act exemptions for this system of records continue to apply to it. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

This system of records notice does not apply to the facilities and perimeters secured by the U.S. Secret Service. Records pertaining to perimeters and facilities secured by the U.S. Secret Service, other than those records subject to the Presidential Records Act, are covered under Department of Homeland Security/U.S. Secret Service-004 Protection Information System of Records, 76 FR 66940, October 28, 2011.

This modified 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 modified system 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-2017-0019 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. 20528-0655.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Jonathan R. Cantor (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS System of Records."

The DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS System of Records covers the collection, use, maintenance, and dissemination of records relating to the protection of property owned, occupied, or secured by DHS. DHS is updating this system of records notice to, among other things, (1) expand the category of individuals to include persons involved in any event, and any witnesses to such event, that affects or impacts the safety, security, or protection of the property, facility, or occupant; (2) remove applicants and contractors who have or had access to classified information as a category of individuals and associated categories of records relating to personnel security because that information has existing coverage under DHS/ALL-023 Department of Homeland Security Personnel Security Management System of Records; (3) add Closed-circuit television (CCTV) recording and audio recordings as categories of records; (4)

add Alien File Numbers, also known as an individual's A-Number as a category of records; (5) modify routine use "E" to be in conformity with Office of Management and Budget Memorandum M-17-12; (6) modify routine use "F" to specifically include Federal Protective Service guards and (7) add a new routine use "M," which will permit DHS to share information with individuals involved in incidents occurring on federal facilities, their insurance companies, and their attorneys for the purpose of adjudicating a claim. This notice also includes non-substantive changes to simplify the formatting and text of the previously published notice. In addition to the existing Privacy Act exemptions that continue to apply to this system of records, DHS is issuing a Notice of Proposed Rulemaking to add a new exemption from certain provisions of the Privacy Act. This 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, and 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/ALL-025 Law Enforcement Authorities in Support of the Protection of Property Owned, Occupied, or Secured by DHS Security Systems of Records.

In accordance with 5 U.S.C. 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-025 Law Enforcement Authorities in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records.

SECURITY CLASSIFICATION: Unclassified, sensitive, for official use only, and classified.

SYSTEM LOCATION: Records are maintained at several DHS Headquarters locations and Component offices, in both Washington, D.C. and field locations.

SYSTEM MANAGER(S): For Headquarters components of DHS: Chief, Physical Security Division (202) 447-5010, Office of Security, Department of Homeland Security, Washington, D.C. 20528. For DHS Components, the System Manager can be found at http://www.dhs.gov/foia under "FOIA Contact Information."

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 40 U.S.C 1315; 44 U.S.C. sec. 3101; and E.O. 9397 as amended by E.O. 13478; E.O. 10450; E.O. 12968, 5 CFR 731; 5 CFR 732; 5 CFR 736; 32 CFR 147; and DCID 6/4.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain and record the results of law enforcement activities in support of the protection of property owned, occupied, or secured by DHS and its components, including the Federal Protective Service (FPS), and individuals maintaining a presence or access to such property. It will also be used to pursue criminal prosecution or civil penalty action against individuals or entities suspected of offenses

that may have been committed against property owned, occupied, or secured by DHS or persons on the property.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include:

- Individuals or entities involved in, or suspected of being involved in, criminal acts against the buildings, grounds, and property that are owned, occupied, or secured by DHS or against persons who are in or on such buildings, grounds, or property. This category includes property located within or outside of the United States;
- Individuals who provide information that is relevant to the investigation, such as victims and witnesses, and who report such crimes or acts;
- Persons involved in any event, or witnesses an event that affects or impacts the safety, security, or protection of the property, facility, or occupant;
- Current, former, or retired DHS personnel who travel outside the United States while employed by DHS.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records in the system may include:

- Individual's or entity's name;
- Alias;
- Digital video recordings and CCTV recordings;
- Audio recordings;
- Date of birth, place of birth, and age;
- Social Security number;
- Alien File Number (A-Number);

- Duty/work address and telephone number;
- Race and ethnicity;
- Citizenship;
- Sex;
- Marital status;
- Identifying marks (e.g., tattoos, scars);
- Height and weight;
- Eye and hair color;
- Biometric data (e.g., photograph, fingerprints);
- Home address, telephone number, and other contact information;
- Driver's license information and citations issued;
- Vehicle information;
- Date, location, nature and details of the incident/offense;
- Alcohol, drugs, or weapons involvement;
- Bias against any particular group;
- Confinement information to include location of correctional facility;
- Gang/cult affiliation, if applicable;
- Release/parole/clemency eligibility dates;
- Foreign travel notices and reports including briefings and debriefings;
- Notices and reports with foreign contacts;
- Reports of investigation;
- Statements of individuals, affidavits, and correspondence;

- Documentation pertaining to criminal activities;
- Investigative surveys;
- Certifications pertaining to qualifications for employment, including but not limited to education, firearms, first aid, and CPR;
- Technical, forensic, polygraph, and other investigative support to criminal investigations to include source control documentation and regional information;
- Data on individuals to include: victims, witnesses, complainants, offenders, and suspects;
- Records of possible espionage, foreign intelligence service elicitation activities, and terrorist collection efforts directed at the Department or its staff, contractors, or visitors;
- Records of close coordination with the intelligence and law enforcement community.

RECORD SOURCE CATEGORIES: Records are obtained from sources contacted during investigations; state, tribal, international, and local law enforcement; and federal departments and agencies.

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. 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) as follows:

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

3. Any employee or former employee of DHS in his/her individual capacity 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. 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 determines that the use of information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist another federal recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) 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; or

2. DHS suspects or has confirmed that there has been a breach of this system of records; and (a) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to DHS (including its information

systems, programs, and operations), the Federal Government, or national security; and (b) 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 contractors and their agents, grantees, experts, consultants, FPS Contract Guard companies, 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, 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 an appropriate federal, state, local, tribal, foreign, or international agency or contract provider, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee or contractor, the issuance of a security clearance, the reporting of an investigation of an employee or contractor, the letting of a contract,

or the issuance of a license, grant, or other benefit, and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or pursuant to the order of a court of competent jurisdiction.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To a federal, state, local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by United States law, E.O., or other applicable national security directive.

L. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

M. To individuals involved in incidents occurring on federal facilities, their insurance companies, and their attorneys for the purpose of adjudicating a claim, such as personal injury, traffic accident, or other damage to property. The release of personal information is limited to that required to adjudicate a claim.

N. 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 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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual name, Social Security number, or other personal identifier listed in "Categories of Records," when applicable.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are pending National Archives and Records Administration approval. DHS has proposed the following retention schedule: Records are maintained in accordance with N1-563-08-4, Item 1. Records are maintained for 20 years after the end of the fiscal year in which the case was closed and are then destroyed. No records will be destroyed until the retention schedule is approved.

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: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the JRA if applicable, because it is a law enforcement system. However, DHS will consider individual requests to determine whether or not information may be released. Thus, 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 and Headquarters or component's FOIA 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, 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 seeking records about yourself from this system of records or any other Departmental 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. In addition, you should:

- 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;

If your request is seeking records pertaining to another living individual, you must, in accordance with 6 CFR 5.21, 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.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, see "access procedures" above.

NOTIFICATION PROCEDURES: See "Record Access procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a (k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the

original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: 75 FR 5614; 74 FR 2903.

Dated: June 8, 2017.

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

[FR Doc. 2017-12262 Filed: 6/13/2017 8:45 am; Publication Date: 6/14/2017]