9110-18

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0007]

Privacy Act of 1974; System of Records

AGENCY: United States Secret Service, Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "Department of Homeland Security/United States Secret Service (USSS)-004 Protection Information System of Records." This system of records describes DHS/USSS collection and maintenance of records on information relative to the protective mission of the agency. In this system of records notice update, DHS/USSS is modifying the categories of individuals, categories of records, routine uses, Authorities, and the retention and disposal of records. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. The Department of Homeland Security previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act. The current updates to this system of records do not impact the nature of the exemptions claimed; the exemptions continue to apply to this update. 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 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-2020-0007 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-2020-0007. 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: E. Gayle Rucker, 202-406-5838, PrivacyServicesProgram@usss.dhs.gov, Privacy Officer, United States Secret Service, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223. For 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

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of

Homeland Security (DHS) United States Secret Service (USSS) proposes to modify and reissue a current DHS system of records titled, DHS/USSS 004 Protection Information System of Records. Information collected in this system of records is used to assist USSS in protecting its designated protectees, events, and venues. In doing so, USSS maintains necessary information to implement protective measures and to make protective inquiries concerning individuals who may come into proximity of a protectee, access a protected facility or event, or who have been involved in incidents or events that relate to the protective functions of USSS. Further, USSS ensures this protective information is appropriately managed and accessible to authorized users while employing appropriate safeguards to ensure that information is properly protected in accordance to national security standards.

DHS/USSS is updating this SORN to:

(1) update the categories of individuals to include individuals who could be in proximity to protected persons or areas secured by USSS;

(2) update the categories of individuals to include persons who fly Unmanned Aircraft Systems (UAS) into areas secured by USSS;

(3) update the categories of records to broaden the name category to include variations of types;

(4) update the categories of records to broaden the address category to an all-inclusive category of Contact Information Identifiers;

(5) update the categories of records to separate confinement and release types from disposition of criminal charges types;

(6) update the categories of records for protective functions to include those related to furthering threat assessment and targeted violence prevention activities, as well as when exercising other USSS protective functions;

(7) update the categories of records to add name check records for credentialing some individuals near protectees;

(8) update the categories of records to include Protective Operations program and management files and Special Event files;

(9) update the categories of records to include citizenship information and identifiers;

(10) update the categories of records to include Government-issued Identifiers of persons;

(11) update the categories of records to include Government-issued Identifiers of property;

(12) update the categories of records to include biometric identifiers and profiles based on biometric attributes;

(13) update the categories of records to include samples of deoxyribonucleic acid DNA and their DNA profiles;

(14) update the routine uses to support USSS's protective function mission to include furthering threat assessment and targeted violence prevention activities;

(15) update the Authorities to include Special Events and the National Threat Assessment Center (NTAC) protective activities;

(16) update the Purpose of System to broaden the activities associated with the agency's protective mission;

(17) update the retention and disposal of records to reflect the most recent National Archives and Records Administration (NARA)-approved records schedules and to include Protective Operations program and management files and Security Events.

Consistent with DHS's information sharing mission, information stored in the DHS/USSS-004 Protection Information 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/USSS 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 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/USSS-004 Protection Information 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)/United States Secret Service (USSS)-004 Protection Information System.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at the USSS Headquarters in Washington, D.C. and field offices. IT Systems covered by this SORN, include E-Check; Protective Intelligence Exchange (PIX); eCASE; and Protective Threat Management System (PTMS); which all can be accessed by individuals located at the United States Secret Service, and 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

SYSTEM MANAGER(S): Assistant Director, Office of Strategic Intelligence and Information; Assistant Director, Office of Technical Development and Mission Support; and Assistant Director, Office of Protective Operations, wfo@usss.dhs.gov, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 18 U.S.C. 3056; 18 U.S.C. 3056A; 18 U.S.C. 871; 18 U.S.C. 879; Presidential Threat Protection Act of 2000, Pub. L. No. 106-544.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is: 1) to assist USSS in protecting its protectees by recording information necessary to implement protective

measures and to investigate individuals who may come into proximity with a protectee or who have sought to make contact with a protectee, as well as individuals who have been involved in incidents or events that relate to the protective functions of USSS; 2) to support field agents coordinating physical security for designated Security Events by providing access to information regarding cases and threat assessments; and 3) to enable USSS to provide assistance to law enforcement officials, school personnel, and others with protective and public safety responsibilities for various types of targeted violence, such as the services provided by the National Threat Assessment Center.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: (1) Individuals who have been or are currently the subject of a criminal investigation by USSS or another law enforcement agency for the violation of certain criminal statutes relating to the safety of persons or security of events, properties, facilities, and areas protected by USSS; (2) Individuals who are subjects of investigative records and reports supplied to USSS by federal, state, and local law enforcement agencies, or private institutions and individuals, in conjunction with the protective functions of USSS; (3) Individuals who are the subjects of non-criminal protective inquiries by USSS and other law enforcement agencies; (4) Individuals who are granted or denied ingress and egress to events, properties, facilities, and areas secured by USSS, or have access to areas in proximity to protected persons or areas secured by USSS, including but not limited to invitees, passholders, tradesmen, law enforcement personnel, maintenance personnel, or service personnel; (5) Individuals who are witnesses, suspects, complainants, informants, defendants, fugitives, released prisoners, and correspondents who have been identified by USSS or from information supplied by other law enforcement agencies, governmental

units, private institutions, and members of the general public in connection with USSS performance of its protective functions; (6) Individuals who fly Unmanned Aircraft Systems (UAS) into protected areas; (7) Individuals who have sought an audience or contact with persons protected by USSS; (8) Individuals who could otherwise be in proximity of protectees or in contact with persons protected by USSS; (9) Individuals who have been involved in law enforcement encounters, incidents or events that relate to the protective functions of USSS; and (10) Individuals who have been or are currently protected by USSS.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Name, alias, or code name;
- Contact information identifiers, such as physical and electronic addresses and phone numbers;
- Date of birth;
- Case number;
- Arrest Record;
- Government-controlled confinement and release information;
- Nature and disposition of criminal charges, to include sentencing and parole or probation status;
- Records concerning agency activities associated with protectee movements and other protective measures taken on a protectee's behalf;
- Records containing information compiled for identifying and evaluating individuals who may constitute a threat to the safety or persons or security of events, properties, facilities, and areas protected by USSS;

- Records containing information compiled for a criminal investigation, including reports of informants and investigators, that are associated with an identifiable individual;
- Records containing reports relative to an individual compiled at various stages of the process of enforcement of certain criminal laws from arrest or indictment through release from supervision;
- Records containing information supplied by other federal, state, and local law enforcement agencies, foreign or domestic, other non-law enforcement governmental agencies, private institutions, and persons concerning individuals who, because of their activities, personality traits, criminal or mental history, or history of social deviancy, may be of interest to USSS in connection with the performance of its protective functions to include furthering threat assessment and targeted violence prevention activities, as well as when exercising other USSS protective functions;
- Records containing information compiled for background investigations, including name check records for credentialing some individuals, including but not limited to, passholders, tradesmen, maintenance, or service personnel who have access and/or have been denied access to areas secured by or who may be in close proximity to persons protected by USSS;
- Records containing information compiled during protective law enforcement encounters in conjunction with National Security Events;
- Records containing information from the Protective Operations program and program files and security event management files;

- Records containing citizenship information and identifiers;
- Records containing information from Government-issued identifiers, including Passport, Social Security, and Driver License Numbers;
- Records containing information from Government-Issued property identifiers, to include boat, vehicle, and UAS registration numbers;
- Records containing information from biometric identifiers and profiles based on biometric attributes to include fingerprint and voiceprint. Such information may be both electronically analyzed and/or examined by human agents; and
- Records containing information from DNA samples and profiles of DNA obtained from the body, such as bodily fluids, or obtained from contacted surfaces. Such information may be both electronically analyzed and/or examined by human agents.

RECORD SOURCE CATEGORIES: The Secretary of Homeland Security has exempted this system from subsections (e)(4)(I) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(2), and (k)(3); therefore, records sources shall not be disclosed.

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 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 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 federal, state, and local governmental agencies for criminal prosecutions; to parole and probation authorities for sentencing and to determine the parole and probation status of criminal offenders or suspected criminal offenders; and to personnel necessary for the completion of civil and other proceedings involving USSS protective functions.

J. To federal, state, and local governmental agencies, foreign and domestic, for the purposes of developing information on subjects involved in USSS protective investigations and the evaluation for and by USSS of persons considered to be of protective interest and for protective functions.

K. To federal, state, and local governmental agencies, foreign and domestic, private institutions and private individuals, for the purposes of designing and implementing protective measures, furthering threat assessment and targeted violence prevention activities, and exercising other USSS protective functions.

L. To private institutions and private individuals, to include identifying information pertaining to actual or suspected criminal offenders or other individuals considered to be of protective interest, for furthering USSS efforts to evaluate the danger such individuals pose to protected persons, facilities, and events.

M. To a court, magistrate, or administrative tribunal in the course of presenting evidence and opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal or civil proceedings.

N. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the 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, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, the issuance of a license, grant, or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

O. 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 that relate to the purpose(s) stated in this SORN.

P. 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/USSS stores records in this system electronically or on paper in secure facilities behind a locked door. The electronic records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/USSS may retrieve records by case number, name, or other identifying data or other case related data in master and magnetic media indices. Access to the physical files is located at field offices, Headquarters, and other Washington, D.C. locations.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Pursuant to NARA Schedule N1-087-11-2, Protective Intelligence Exchange System (PIX), protective intelligence case records, including non-judicial protective intelligence cases, are routinely retained for a period of up to 5 years from the date of last action; or for 10 years from the date of last action if they contain electronic

records. All judicial records are retained for a period of 30 years from the date of last action, unless otherwise required to be held permanently for transfer to NARA. Files relating to issuance of White House Complex passes for employees of the White House, USSS employees, press representatives accredited at the White House, and other authorized individuals are retained for a period of 8 years from the date the file is closed.

Video surveillance source data from cameras and protectee active location data is maintained for 30 days. Recordings relevant to an investigative inquiry are retained for a minimum of 3 years following the date recorded but can be kept with a relevant case file. Video recordings associated with a highly unusual incident, occurrence, or significant event are permanent and are subsequently transferred to NARA when 25 years old.

Planning and after-action records pertaining to Presidential inaugurations and campaign records related to a Presidential candidate not currently under Secret Service protection are permanent and are subsequently transferred to NARA when 25 years old. Routine records pertaining to the administration and operations of USSS protective programs, logs, shift reports, survey files and related documents/data, and trip reports are retained for a period of 3 years up to 10 years, from the end of the event. Non-Criminal Protective Investigation Name Check Reports are kept until no longer needed, e.g., cut off at end of the month, and destroyed 30 days after cutoff, as approved in its NARA Schedule.

Special Event files not related to an inauguration are retained for 5 years. In the event of a highly unusual protective incident – e.g., assassination attempt, successful assassination, or events requiring extraordinary protective measures – relevant records of

the incident, including those normally scheduled as temporary, will be retained and subsequently transferred to NARA 25 years after the incident.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/USSS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/USSS 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 the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether information may be released. 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 USSS 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: This system of records is exempt from the Privacy Act's access and amendment provisions and those of the Judicial Redress Act; therefore, record access and amendment may not be available. In such cases, certain records about you may be available under the FOIA, and the correspondence from those seeking a record amendment may be placed in the respective case file. 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.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 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), (e)(12); (f); (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(1), (k)(2), and (k)(3), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. sec. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When this system receives a record from another system exempted in that source system under 5

U.S.C. sec. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary system of records from which they originated and claims any additional exemptions set forth here.

HISTORY: DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011); Implementation of Exemptions, DHS/USSS-004 Protection Information System of Records, 74 FR 45090 (August 31, 2009).

Constantina Kozanas,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2020-22534 Filed: 10/9/2020 8:45 am; Publication Date: 10/13/2020]