

9111-28

**DEPARTMENT OF HOMELAND SECURITY**

Docket No. DHS-2018-0069

**Privacy Act of 1974; System of Records**

**AGENCY:** Department of Homeland Security, U.S. Immigration and Customs Enforcement.

**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/U.S. Immigration and Customs Enforcement (ICE) system of records titled, “Department of Homeland Security/U.S. Immigration and Customs Enforcement-017 Angel Watch Program System of Records.” This system of records covers records collected as part of ICE’s Angel Watch Program (also referred to as Operation Angel Watch) conducted by the Child Exploitation Investigations Unit of the ICE Homeland Security Investigations Cyber Crimes Center. ICE’s Angel Watch Program is conducted as part of the Angel Watch Center (AWC), a joint initiative among ICE, DHS’s U.S. Customs and Border Protection (CBP), and the U.S. Department of Justice’s U.S. Marshals Service, as prescribed by International Megan’s Law (IML) to Prevent Child Exploitation and Other Sexual Crimes through Advanced Notification of Traveling Sex Offenders (Public Law 114-119).

The AWC’s mission is to prevent child sex tourism by alerting destination countries that covered sex offenders – individuals who have been convicted of sexual offenses against minors and are required to register as sex offenders with any jurisdiction in the United States – have scheduled upcoming travel to those countries. In accordance

with IML, the AWC sends information to the U.S. Department of State (DoS) to facilitate that agency's placement of unique identifiers on the passports of covered sex offenders.

This system of records describes how DHS/ICE, in accordance with IML, collects and maintains records about covered sex offenders and shares certain information with DoS; the U.S. Department of Justice; other federal, state, and local agencies; and foreign countries. This newly established system of records 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 new system will be effective upon publication. 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-2018-0069 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: Philip S. Kaplan, 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-2018-0069. 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: Amber Smith, (202) 732-3300, Privacy Officer, Office of Information Governance and Privacy, Immigration and Customs Enforcement, 500 12<sup>th</sup> Street, S.W., Mail Stop 5004, Washington, D.C. 20536. For privacy questions, please contact: Philip S. Kaplan, privacy@hq.dhs.gov, (202) 343-1717, 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), U.S. Immigration and Customs Enforcement (ICE) proposes to establish a new DHS system of records titled, “DHS/ICE-017 Angel Watch Program System of Records.” This system of records covers only Angel Watch Program activities (also referred to as Operation Angel Watch) conducted by the Child Exploitation Investigations Unit of the ICE Homeland Security Investigations (HSI) Cyber Crimes Center, which developed the Angel Watch Center (AWC), a joint initiative among ICE, DHS’s U.S. Customs and Border Protection (CBP), and the U.S. Department of Justice’s U.S. Marshals Service, as prescribed by International Megan’s Law (IML) to Prevent Child Exploitation and Other Sexual Crimes Through Advanced Notification of Traveling Sex Offenders (Public Law 114-119).

ICE previously relied on the DHS/ICE-009 External Investigations System of Records Notice, last published at 75 FR 404 (January 5, 2010), to cover Angel Watch Program records. ICE has determined a separate system of records notice (SORN) will

provide greater transparency and clearly describe the records the Angel Watch Program collects and maintains on individuals.

This system of records does not cover records originating from Justice/FBI-001 National Crime Information Center (NCIC) System of Records;<sup>1</sup> DHS/CBP-006 Automated Targeting System;<sup>2</sup> and the U.S. Department of State Consular Lookout and Support System.<sup>3</sup> At all times, the Angel Watch Program references these records directly from the underlying systems in a manner consistent with law enforcement purposes stated in the source systems' compliance documentation.

This system of records also does not cover CBP or U.S. Marshals Service records created or maintained as part of their work in the AWC. Additionally, in some cases, records originating with Angel Watch Program activities may give rise to or be used in investigations by ICE. Those records continue to be covered by the DHS/ICE-009 External Investigations SORN.

The Angel Watch Program, created in 2007 by ICE's HSI, and managed by the Child Exploitation Investigations Unit of HSI's Cyber Crimes Center, identifies individuals who have been convicted of sexual crimes against a minor and who may be traveling overseas for the purpose of sexually abusing or exploiting minors, a crime known as "child sex tourism," and notifies the relevant destination countries, as appropriate.

---

<sup>1</sup> JUSTICE/FBI 001–National Crime Information Center, 64 FR 52343 (September 28, 1999), and as amended, available at: <https://www.justice.gov/opcl/doj-systems-records>.

<sup>2</sup> DHS/CBP 006–Automated Targeting System, 77 FR 30297 (May 22, 2012).

<sup>3</sup> STATE 05–Overseas Citizen Services Records, September 8, 2016, 81 FR 62235 (September 8, 2016); STATE 26–Passport Records, March 24, 2015, 80 FR 15653 (March 24, 2015); and STATE 39–Visa Records, October 25, 2012, 8377 FR 28062 (June 15, 2018). U.S. Department of State SORNs are available at: <https://www.state.gov/privacy/soms/index.htm>.

Additionally, the AWC is required to provide the U.S. Department of State (DoS) with information about covered sex offenders – individuals who have been convicted of sexual offenses against minors and are required to register as sex offenders with any jurisdiction in the United States – who are traveling or intend on traveling abroad so DoS may place a unique identifier on their U.S. passports.

Pursuant to IML, the Angel Watch Program runs automated queries through CBP's Automated Targeting System – Passenger (ATS-P). ATS-P scans passenger manifests of outgoing international flights and identifies passengers with a possible match to a record in the National Sex Offender database owned by the Department of Justice's National Criminal Information Center (NCIC) for a sexual offense against a minor (hereinafter, National Sex Offender Registry or NSOR). Once a traveler is identified as a potential match to an NSOR record, the Angel Watch Program reviews the traveler's biographical data received from ATS-P to verify that the traveler is correctly matched to the subject identified in the NSOR record, and also reviews the corresponding NCIC criminal history data to confirm that the traveler has been convicted of a covered sex offense as defined within IML. In accordance with information sharing agreements, once the Angel Watch Program has confirmed individuals with scheduled travel are covered sex offenders, it shares information about those individuals with the U.S. Marshals Service, which is co-located at the AWC, to ensure the covered sex offenders have provided notification to states or locales about their upcoming travel, as applicable. As part of the Angel Watch Program, ICE does not use or retain any information about individuals who are determined not to be covered sex offenders.

Through the Angel Watch Program ICE evaluates multiple factors including the details of each covered sex offender's travel itinerary to determine if notification to the destination country is appropriate. If ICE determines that notification is appropriate, it sends an operational record (i.e., biographic information from source systems pertaining to a covered sex offender) to HSI Attaché offices, which are located at certain United States embassies. The Attachés then send a notification record (i.e., a derivative of an operational record containing only the information needed to provide situational awareness) to law enforcement and/or border security officials in the destination country or countries of the covered sex offender's pending arrival. By notifying officials in the destination countries prior to the covered sex offender's arrival, and by providing basic flight information and conviction information located in the NSOR, HSI enables the destination countries to make informed decisions about whether they believe the covered sex offender may pose a risk of engaging in child sex tourism. HSI advises foreign countries that this information is for informational purposes only. If ICE's Angel Watch Program determines that notification is inappropriate, it will not proceed and will delete the information.

Prior to traveling abroad, ICE strongly encourages travelers who believe they might be a covered sex offender to contact the destination country to ensure they will be permitted entry upon arrival.

In accordance with 34 U.S.C. 21503(e)(7), ICE's Angel Watch Program has established a mechanism to receive complaints from individuals alleged to be affected by erroneous notifications to destination countries. The Angel Watch Program will ensure that any complaint is promptly reviewed, and in the case of a complaint that involves a

notification sent by another Federal Government agency, the Angel Watch Program will provide the individual with the contact information, for the appropriate entity and forward the complaint to that entity, as required by IML. If the Angel Watch Program determines it provided inaccurate information, it will take corrective action to remedy the error, including notifying any foreign government who received the inaccurate information, as well as other Federal Government agencies with which it has previously shared the incorrect information, so they can update their records, as needed. The Angel Watch Program will provide a complainant with a written response in the event incorrect information was shared, along with an explanation, to the extent permitted by law and policy, as to why the incorrect information was shared, and actions the program has taken to remedy the error. The Angel Watch Program will publicly post instructions on how to submit a complaint on the ICE public-facing website. The program agrees to receive any complaint about an individual having been identified by the Angel Watch Program as a covered sex offender via email at the following address:

[DHSINTERMEGANSLAW@ICE.DHS.GOV](mailto:DHSINTERMEGANSLAW@ICE.DHS.GOV).

This new system of records 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/ICE-017 Angel Watch Program System 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)/U.S. Immigration and Customs Enforcement (ICE)-017 Angel Watch Program System of Records.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Records are maintained at the ICE Headquarters in Washington, D.C. and Homeland Security Investigations (HSI) Attaché offices abroad.

**SYSTEM MANAGER(S):** Homeland Security Investigations, Cyber Crimes Center Child Exploitation Investigations Unit, (866) 347-2423, U.S. Immigration and Customs Enforcement, 500 12th Street S.W., Washington, D.C. 20536

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 6 U.S.C. 202-203; 18 U.S.C. 1591, 1596, 2251, 2260, 2423; 19 U.S.C. 1628, 34 U.S.C. 21503.

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to collect information on covered sex offenders to: (1) Combat transnational child sex tourism or exploitation; (2) Share information on covered sex offenders with foreign countries to aid them in making informed decisions regarding the admissibility of travelers in their own countries; (3) Support the receipt of and response to any complaints by alleged covered sex offenders or others related to the activities of the Angel Watch Program; (4) Identify potential criminal activity; uphold and enforce criminal laws; and ensure public safety.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Categories of individuals covered by this system are: (1) individuals, including United States citizens, who have an NSOR record for a sexual offense against a minor and who have scheduled international travel, and (2) individuals, as well as any representative acting on their behalf, filing complaints with the Angel Watch Program concerning alleged inaccurate information.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Categories of records in this system include:

1. Notification records consist of information transmitted to DHS's foreign counterparts for situational awareness. This information may include name, date of birth, Alien Registration Number (A-Number), Social Security number, passport number, and country of birth.

2. Complaints filed by individuals or their representatives concerning the sharing of their travel information under this program. This includes any information submitted by the complainant; information compiled by the agency in researching the complaint; records of an individual's criminal history and/or status on the sex offender

registry; memoranda or other communications within the agency or with other agencies related to the complaint; research conducted in DHS and other government data systems; and the agency's response to the complaint.

**RECORD SOURCE CATEGORIES:** Angel Watch Program notification records validate biographic information against the Advance Targeting System – Passenger (ATS-P), owned by U.S. Customs and Border Protection;<sup>4</sup> the National Sex Offender Registry within the National Crime Information Center, maintained by the Federal Bureau of Investigation;<sup>5</sup> domestic courts and law enforcement agencies; the U.S. Department of Justice's National Sex Offender Public Website (NSOPW), and state, territories, and tribal sex offender registries, available through NSOPW, including the entities responsible for their maintenance;<sup>6</sup> and the U.S. Department of State from its Consular Lookout and Support System.<sup>7</sup> Information is also obtained directly from the individuals covered by this system of records or their representatives in the event a complaint is filed.

**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

---

<sup>4</sup> DHS/CBP 006–Automated Targeting System, 77 FR 30297 (May 22, 2012).

<sup>5</sup> JUSTICE/FBI 001–National Crime Information Center, 64 FR 52343 (September 28, 1999), and as amended, *available at*: <https://www.justice.gov/opcl/doj-systems-records>.

<sup>6</sup> NSOPW is a public resource that searches the public sex offender registries from all 50 states, the District of Columbia, the five principal U.S. territories, and federally recognized Indian tribes. Conversely, the FBI's National Sex Offender Registry is a database available only to law enforcement that is maintained by the FBI's Criminal Justice Information Services Division.

<sup>7</sup> STATE 05–Overseas Citizen Services Records, September 8, 2016, 81 FR 62235 (September 8, 2016); STATE 26–Passport Records, March 24, 2015, 80 FR 15653 (March 24, 2015); and STATE 39–Visa Records, October 25, 2012, 8377 FR 28062 (June 15, 2018). Department of State SORNs are *available at*: <https://www.state.gov/privacy/sorns/index.htm>.

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 U.S. Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agencies 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 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 a foreign government to provide notice of the intended travel of a covered sex offender from the United States to the foreign country, and to assist that government in making an informed decision as to whether the offender may pose a risk of engaging in child sex tourism while in that country.

J. To federal, state, tribal, territorial, local, international, or foreign government agencies or entities for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) to verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) to verify the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

K. To the U.S. Marshals Service to coordinate, cooperate, and de-conflict activities related to the foreign travel of covered sex offenders.

L. To the U.S. Department of State: (1) to provide notice of U.S. citizens identified as covered sex offenders who are traveling, or intend on traveling, abroad so Department of State may place a unique identifier on their passports; (2) to provide notice of those individuals no longer deemed a covered sex offender; or (3) to resolve complaints, inaccuracies, or errors.

M. To other Federal Government agencies for the purpose of referring complaints received from individuals that are appropriately handled by those other agencies.

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/ICE 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 name and/or name and date of birth. In the case of complaints, records may be retrieved by name or complaint number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** ICE is in the process of drafting a proposed record retention schedule to be submitted to NARA for approval for the information maintained by the Angel Watch Program. The proposed retention policy for notification records is seven (7) years from the year in which the travel was scheduled to occur, and for complaint records, seven years after the complaint was closed.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** DHS/ICE safeguards records in this system according to all applicable rules and policies, including all applicable DHS automated systems security and access policies. ICE has 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 may submit a request in writing to the Chief Privacy Officer and ICE Freedom of Information Act (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 provides 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. 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 you believe the Department would have information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about him/her;
- 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 an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

Without this bulleted 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. Individuals who wish to contest the accuracy of records in this system of records should submit these requests to the Privacy Division of the ICE Information Governance & Privacy Office. Requests must comply with verification of identity requirements set forth in Department of Homeland Security Privacy Act regulations at 6 CFR 5.21(d). Please specify the nature of the complaint and provide any supporting documentation. By mail (please note substantial delivery delays exist): ICE Information Governance & Privacy Office, ATTN: Privacy Division, 500

12th Street S.W., Mail Stop 5004, Washington, D.C. 20536. By email:

ICEPrivacy@ice.dhs.gov.

Please contact the Privacy Division with any questions about submitting a request at 202-732-3300 or ICEPrivacy@ice.dhs.gov.

**NOTIFICATION PROCEDURES:** See “Record Access Procedures”.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** None.

Philip S. Kaplan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2019-00770 Filed: 1/31/2019 8:45 am; Publication Date: 2/1/2019]