Privacy Impact Assessment

for the

Angel Watch Program

DHS Reference No. DHS/ICE/PIA-057

August 10, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operates the ICE Angel Watch Program (AWP). The AWP mission is to proactively identify individuals who have been convicted of sexual crimes against children and have upcoming travel to a foreign country, in order to notify law enforcement and/or border security in the destination country. In 2016, AWP was codified by the International Megan's Law to Prevent Child Exploitation and Other Sexual Crimes through Advanced Notification of Traveling Sex Offenders (International Megan's Law or IML).[1] This Privacy Impact Assessment (PIA) assesses the privacy risks presented by AWP's operations, including its disclosures to U.S. Government agencies and foreign law enforcement and border security agencies, under IML.

Overview

The Angel Watch Center (AWC), which administers the AWP, is led by the ICE Office of Homeland Security Investigations (HSI) Cyber Crimes Center (C3) in coordination with the U.S. Customs and Border Protection (CBP) National Targeting Center (NTC) and the U.S. Marshals Service (USMS) National Sex Offender Targeting Center (NSOTC). The purpose of the AWP is to identify U.S. citizens (USC) and lawful permanent residents (LPR) (collectively referred to as U.S. persons) who (1) have a conviction for a sexual crime against a child and (2) have upcoming international travel.

After identifying individuals who meet the IML definition of covered sex offender who have upcoming international travel, AWP notifies foreign law enforcement or border security officials in the destination countries of the covered sex offenders' upcoming travel either via HSI Attaché or CBP liaison offices. The notification (also known as referral) serves to:

- Reduce the risk of U.S. persons engaging in child sex tourism in foreign countries;
- Enable foreign countries to make fully informed decisions relating to admissibility, border inspections, surveillance or investigative measures, or any other action deemed appropriate with respect to the covered sex offender; and
- Encourage foreign countries to provide the United States with notifications when foreign nationals convicted of sexual crimes against children are traveling to the United States.[2]

Identification of Covered Sex Offenders and Determination of Whether to Notify Foreign Counterparts

[1] International Megan's Law to Prevent Child Exploitation and Other Sexual Crimes through Advanced Notification of Traveling Sex Offenders, Pub. L. No. 114-119, 130 Stat 15 (2017) (current version at 22 U.S.C. § 212b).
[2] Reciprocal notifications for foreign offenders (i.e., non-U.S. persons) traveling to the United States are received under the AWP, but very seldom. AWP averages less than a half-dozen notification receipts per year. When such notifications are received, the information is provided to CBP for appropriate action when encountering the non-U.S. person or USMS for sex offender registry purposes.

The Aviation and Transportation Security Act (ATSA) of 2001[3] and the Enhanced Border Security and Visa Reform Act of 2002[4] mandated the collection of information on all passengers and crew members who arrive in or depart from (and, in the case of crew members, overfly) the United States on a commercial air or sea carrier, in addition to individuals aboard a private aircraft arriving in or departing from the United States. As a result of the 9/11 Commission recommendations, Congress mandated, through the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), that DHS establish a requirement to receive advance passenger information (API) on passengers traveling internationally prior to their departure.[5] The information collected (generally in the form of a flight or vessel/ship manifest) can generally be found on routine travel documents that passengers and crew members must provide to CBP when attempting to enter or depart the United States. A passenger manifest that is sent to CBP's Advance Passenger Information System (APIS)[6] typically includes:

- Full name;
- Date of birth (DOB);
- Citizenship;
- Alien registration number;
- Travel document type and travel document information; and
- U.S. destination address (when applicable).

AWP personnel (i.e., HSI and CBP analysts) use information maintained in DHS databases and other federal government databases (e.g., National Crime Information Center (NCIC) National Sex Offender Registry (NSOR)[7]) to identify passengers who have a conviction for a sexual crime against a child. The AWP personnel are responsible for vetting all positive matches to verify that the passenger is the covered sex offender in question. AWP personnel conduct a manual comparison of the available API, NSOR record, Department of State (DOS) Consular Consolidated Database (CCD)[8] U.S. passport information, any other U.S. Government data source,

[3] Aviation and Transportation Security Act of 2001, Pub. L. No. 107-71, 115 Stat 597 (2001) (current version at 49 U.S.C.).
[4] Enhanced Border Security and Visa Reform Act of 2002, Pub. L. No. 107-173, 116 Stat 543 (2002) (current version at 8 U.S.C.).
[5] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat 3638 (2004) (current version at 50 U.S.C.).
[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS), DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[7] The National Sex Offender Registry database is owned by the Department of Justice's (DOJ) National Criminal Information Center (NCIC). *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION NATIONAL CRIMINAL INFORMATION CENTER (NCIC), *available at* https://www.fbi.gov/services/cjis/ncic (last visited August 9, 2020).
[8] CCD is the official repository of visa and passport information. For additional information, s*ee* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (2018), *available at* https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf.

and/or other publicly available open-source information. If additional information is required during the vetting process, HSI analysts may use ICE's Investigative Case Management (ICM) system[9] as a secondary check to verify the covered sex offender's criminal history record. Once AWP personnel confirm that the offender has been convicted of a "covered sex offense" as defined by IML, the AWP will notify the HSI Attaché/CBP liaison office responsible for coordinating with the destination country's designated law enforcement entity. If the offender was convicted for a "covered sex offense" and is required to register anywhere in the United States, notification will be sent to USMS for verification and DOS for the required IML marking.

Information Sharing and Notification/Referral Process

AWP's notifications are not an effort to restrict the covered sex offender's travel, generate an arrest for every notification, or monitor all activities of the covered sex offender. Rather, these notifications are designed to inform the destination countries of a covered sex offender's upcoming travel for situational awareness. AWP considers existing information sharing agreements with the destination countries as the standard for determining whether notification is warranted. In cases where the AWP determines that a notification is warranted, the covered sex offender's information is provided to the following entities:

1. USMS NSOTC via encrypted email to verify that the covered sex offender is in compliance with all state and/or federal sex offender registration requirements;
2. The appropriate HSI Attaché/CBP liaison office in the destination country to transmit the notification to the appropriate foreign law enforcement or border patrol agency in the destination country;[10] and
3. The DOS Bureau of Consular Affairs via encrypted email, for passport endorsement (i.e., marking the covered sex offender's passport), as required by IML.

Per IML, any notification made to a foreign country through the AWP must first be provided to USMS to confirm registration requirements if the covered sex offender is identified more than 24 hours before departure. For covered sex offenders identified less than 24 hours before departure, notification may be sent to USMS and the HSI Attaché/CBP liaison office simultaneously. The referral to USMS and the HSI Attaché/CBP liaison office contains the following information:

- Full name;
- Date of birth (DOB);

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-045 (2016), *available at* https://www.dhs.gov/privacy-documents-ice. ICM is not used for maintaining records of each AWC referral.
[10] The AWP sends the covered sex offender's information to the appropriate HSI Attaché/CBP liaison office which then shares a subset of the information with relevant foreign law enforcement officials through whatever information sharing protocols they have in place.

- U.S. passport number or other travel document;
- Country of birth (COB);
- Social Security Number;
- Alien Registration Number;
- Conviction and sex offender registry information including, the sexual offense, date of conviction, and the age of the victim,[11] if available; and
- Travel itinerary and travel document information.

The HSI Attaché/CBP liaison office considers the varying legal authorities and working relationships in the destination country and provides notification to foreign law enforcement and/or border patrol agency containing a subset of the information in the referral it received from the AWP (i.e., only the information needed for the in-country official to identify and locate the covered sex offender for any further action they deem appropriate). HSI does not make any recommendation as to whether the covered sex offender should be granted entry into the destination country, but rather provides the information for situational awareness purposes. Any action taken as a result of the information is made solely by the receiving country in accordance with its own laws.

Finally, the AWP provides the DOS Bureau of Consular Affairs with biographic data for covered sex offenders with a verified registration requirement in any U.S. jurisdiction, where they have a current U.S passport that does not bear the required IML child sex offender endorsement.[12] In these cases, the current passports issued to these offenders are revoked by DOS. Once revoked, DOS provides the offenders with an official letter informing them of the revocation and that they may apply for a new passport bearing the required endorsement.

Erroneous Notifications Complaints Process

In accordance with IML, the AWP has established a mechanism to receive complaints from individuals alleged to be affected by erroneous notifications to destination countries or to DOS for passport revocations. The AWP will ensure that any complaint is promptly reviewed, and in cases where the complaint directly pertains to information originating from another U.S. Government agency (e.g., CBP, USMS, DOS), the AWP will forward the complaint to that agency and will provide the individual with relevant contact information. If the AWP determines that it provided inaccurate information, the center will take corrective action to remedy the error, including notifying any foreign government that received the inaccurate information, as well as any other U.S. Government agencies with which it has previously shared the incorrect information. This is

[11] No other personal information about the victim is shared in the notification.
[12] Verification is made once USMS confirms the offender's registration requirements with the local sex offender registry.

performed so that these parties can update their records, as needed. In addition, the AWP will provide the complainant with a written response stating that incorrect information was shared, along with an explanation, to the extent permitted by law and policy, stating the reason for which the incorrect information was shared, and all actions taken by the AWP to remedy the error.

The published AWP System of Records Notice (SORN) provides instructions on how to submit complaints regarding the AWP.[13] The AWC will receive any complaint related to an individual being identified as a covered sex offender via email, dhsintermeganslaw@ice.dhs.gov.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[14] articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[15]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[16] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. This PIA is conducted as it relates to the DHS construct of the FIPPs and examines the privacy impact of the AWP.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.*

---

[13] DHS/ICE-017 Angel Watch Program System of Records, 84 Fed. Reg. 1182 (March 4, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] 5 U.S.C. § 552a.
[15] 6 U.S.C. § 142(a)(2).
[16] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.

As authorized by statute,[17] and in support of HSI's mission to combat child sex trafficking and tourism, the AWP identifies U.S. persons who have been convicted of a sexual offense involving a minor in the United States, who are required to register as a sex offender in any state or territory of the United States as the result of such conviction, and who have upcoming international travel. Once the AWP determines notification is warranted, the offender's information is provided to USMS; the appropriate HSI Attaché/CBP liaison office; DOS; and in turn, to foreign law enforcement in the destination country. Information collected from publicly available sources and U.S. Government agency source systems and shared about these individuals is in accordance with the AWP established (i) law enforcement purpose and (ii) business processes. ICE also provides general notice to individuals about the collection and sharing of their information in accordance with approved legal authorities through privacy compliance documentation (such as this PIA and associated SORN). Furthermore, ICE informs individuals about the role of AWP in news releases on the ICE public website.[18]

Privacy Risk: There is a risk that individuals will not have adequate notice that their information is collected and shared with other parties.

Mitigation: This risk is partially mitigated. ICE is providing detailed notice to the public regarding the AWP's operations through the publication of this PIA, including AWP's use of PII to identify covered sex offenders and to determine whether to notify foreign counterparts. Furthermore, the DHS/ICE-017 Angel Watch Program SORN provides notice regarding the records maintained by the AWP and establishes the routine uses enabling the AWP's disclosures to USMS, DOS, and destination countries' law enforcement/border patrol agencies.[19] ICE also provides information about AWP on its public-facing website.

However, because of the law enforcement nature of the AWP, notice is not provided directly to individuals.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and*

[17] DHS has been authorized to collect information under 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; and IML.
[18] "ICE authorized to create Angel Watch Center to expand child protection efforts following passage of International Megan's Law" (February 9, 2016), *available at* https://www.ice.gov/news/releases/ice-authorized-create-angel-watch-center-expand-child-protection-efforts-following, and "ICE HSI opens Angel Watch Center to combat child sex tourism, announces FY19 child exploitation investigative results" (November 14, 2019), *available at* https://www.ice.gov/news/releases/ice-hsi-opens-angel-watch-center-combat-child-sex-tourism-announces-fy19-child.
[19] DHS/ICE-017 Angel Watch Program System of Records, 84 Fed. Reg. 1182 (March 4, 2019), specifically routine uses G, I, K, and L.

maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Due to the law enforcement purpose of the AWP, individuals do not have an opportunity to consent or opt-out of the program's collection and use of their information from publicly available sources and U.S. Government agencies' source systems. A U.S. person may request access, correction, and redress with respect to the notification sent by the HSI Attaché/CBP liaison office to a foreign government, as the notification is the only record created by the AWP. The AWP will not process requests by U.S. persons to access or correct the source system data used to create that notification. Any such requests for access to or correction of source system data should be made to the relevant U.S. Government agency Privacy or Freedom of Information Act (FOIA) Office (i.e., CBP, USMS, or DOS) as the data owner.

Privacy Risk: There is a risk that individuals may not be provided redress if the AWP shares inaccurate information.

Mitigation: This risk is mitigated. The AWP will coordinate and share information with other federal agencies, as appropriate, to respond to and resolve complaints where each agency has equities or responsibilities. For example, the AWP will direct a complainant to CBP for a request related to incorrect information maintained in CBP system(s). In addition, the AWP will work with the ICE point of contact for the DHS Traveler Redress Inquiry Program (TRIP)[20] to establish a process that ensures individuals who contact DHS TRIP claiming to have been misidentified as covered sex offenders, are promptly referred to the AWP. For AWP-specific requests, the AWP has established a comprehensive review process for individuals seeking access, correction, and redress regarding the notifications that the AWP sends to foreign governments and to the DOS for the IML passport endorsement. The AWP receives complaints from the public via email at dhsintermeganslaw@ice.dhs.gov and describes the process for submitting such a complaint in both this PIA and the AWP SORN. The AWP will provide an automated response to emails sent to dhsintermeganslaw@ice.dhs.gov, which will, at a minimum, contain the following:

- Basic information about the AWP's mission and legal authority to make disclosures consistent with IML;
- Specific instructions about how to submit claims that the AWP has shared inaccurate information with a foreign government;
- A link to the ICE public-facing website containing the Certification of Identity and Privacy Waiver forms;[21]

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM (TRIP), DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[21] DHS Form 500-05: Certification of Identification" and ICE Form 60-001: Privacy Waiver for Authorizing Disclosure to a Third Party, *available at* https://www.ice.gov/privacy.

- Instructions on how to contact DOS for issues involving passports (e.g., for individuals with marked passports who no longer have a registration requirement); and
- A clear statement that the AWP does not process individual or third party (acting on an individual's behalf) requests to stop sending notifications to destination countries when that individual is required to register with the jurisdiction's sex offender registry.

The AWP will adjudicate and respond to claims stating that AWP shared inaccurate information within 90 days of receiving all required documentation from the complainant. The AWP will make reasonable efforts to research an individual's claim, such as checking available public and government databases. If the AWP concludes that the information shared about the individual was not accurate, the AWP will immediately notify the following parties with a description of the inaccuracy and a request to correct their records and take any additional, relevant actions, as appropriate:

- DOS Bureau of Consular Affairs, Office of Passport Services (CA/PPT), for the purposes of reviewing and reissuing passports;[22]
- USMS for the purposes of correcting its records and contacting previously notified destination countries;[23] and/or
- The ICE HSI Attaché/CBP liaison office to whom the AWP sent inaccurate information, so that the HSI Attaché/CBP liaison office may relay accurate information to the destination country.

In addition, the AWP will send an email to the complainant with the following elements in a password-protected PDF attachment (with the password sent in a second email):

- An acknowledgment that the AWP sent an inaccurate notification about the individual;
- An explanation containing the reason why the AWP sent inaccurate information about the individual to the destination country, to the extent permitted by law and policy;[24] and
- Notice that AWP has contacted DOS to reach out to the complainant directly with information about passport reissuance.

Where there is insufficient evidence showing that the notification was inaccurate, the AWP will send an email to the complainant with a password-protected PDF attachment (with password sent in a separate email) containing information that the claim of inaccuracy has been denied and the relevant procedures in place to request a review of the program's determination. If a complainant

[22] AWC will send a notification to npic@state.gov. If a passport is revoked due to an error, there will not be any cost passed to the individual. DOS will simply issue them a new passport.
[23] In this case, AWP would send a notification to NSOTC.IML@usdoj.gov.
[24] For example, inaccurate information about the individual in U.S. Government holdings.

requests a review of the AWP's determination, that review will be handled by the Privacy Unit of the ICE Office of Information Governance and Privacy (IGP).

Lastly, if, upon review, the Privacy Unit concurs with the AWP's determination to deny the complainant's claim of inaccuracy, the Privacy Unit will notify the individual and provide information on the administrative appeals process. If the complainant files an administrative appeal with ICE in response to the Privacy Unit's determination, as provided for under subsection (d)(3) of the Privacy Act of 1974, the AWP will, until such time that the dispute is resolved, note in any future disclosures that the complainant has disputed the accuracy of the information, and will include a copy of the individual's statement with each disclosure. The AWP may also include a concise statement of the reasons that the agency did not grant the requested amendment.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

DHS has been authorized to collect information for the AWP under 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; and IML. These statutes establish the purpose of AWP, which is to identify covered sex offenders who have upcoming international travel and, as applicable, notify domestic and foreign law enforcement or border security officials in an effort to: (1) reduce child sex tourism in foreign countries; (2) enable foreign countries to make fully informed decisions relating to the admissibility, border inspections, surveillance or investigative measures, or any other action deemed appropriate with respect to the covered sex offender and that country's applicable laws; and (3) increase information sharing to encourage foreign countries to provide the United States with notifications when foreign nationals convicted of sexual crimes against children in their countries are traveling to the United States. To fulfill its statutory mission, the AWP collects, uses, and discloses PII maintained in other DHS and U.S. Government databases, and publicly available sex offender websites.

Privacy Risk: There is a risk that foreign law enforcement partners will use the information for purposes that are not authorized under the statutes and regulations listed above.

Mitigation: This risk cannot be fully mitigated. However, ICE has taken a number of steps to mitigate misuse. Information that is shared with foreign law enforcement partners is limited to information that helps provide situational awareness. The notifications sent by the HSI Attaché/CBP liaison office to destination country governments provide only the information needed for the destination country official to determine if further action is deemed appropriate and to identify and locate the sex offender. Furthermore, the HSI Attaché/CBP liaison office reviews the AWP referrals and determines whether the content in the notification sent to the destination country is appropriate. The HSI Attaché/CBP liaison office also provides a briefing to destination country authorities to help them understand the AWP's purpose and the extent of its mission. This includes the creation of protocols to help ensure that the destination country's authorities manage

the notification information in compliance with U.S. law, the destination country's law, and other binding agreements (e.g., Customs Mutual Assistance Agreements).

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

As stated previously, AWP personnel compare API with NSOR records to identify international travelers who have previously been convicted of sexual crimes against children prior to departure. Once identified, on a case-by-case basis, AWP personnel determine whether notification to the destination country's government is warranted. In cases where the AWP determines that a notification is warranted, as established in IML, the covered sex offender's information is provided to: (1) USMS to verify that the covered sex offender is in compliance with all state or local sex offender registration requirements; (2) the appropriate HSI Attaché/CBP liaison office to transmit a notification to the appropriate foreign law enforcement or border patrol agency in the destination country; and (3) the DOS Bureau of Consular Affairs for passport endorsement. In turn, the HSI Attaché/CBP liaison office provides only the information needed for an in-country official to identify and locate the offender and to assess if further action is deemed appropriate. The notification to the destination country is only informational. It does not advise on whether to permit or deny the offender's entry, as foreign countries have sovereignty.

In addition, although the AWP records are currently unscheduled and must be retained indefinitely until a record schedule is approved by the National Archives and Records Administration (NARA), ICE will be proposing a seven-year retention policy for notification records (i.e., from the date in which the travel was scheduled to occur) and a seven-year retention policy for complaint records (i.e., after the complaint has been closed). Following the seven-year timeframe, AWP will destroy these records.

Privacy Risk: There is a risk that AWP information is retained longer than necessary to accomplish the purpose for which it was originally collected.

Mitigation: This risk is not currently mitigated. ICE has determined that the proposed seven-year retention period is adequate to fulfill the purposes of the AWP and does not increase the risk of misuse or disclosure of the information. A retention period of seven years is based on the operational needs of the program and legal needs of the individual. The retention policy applies regardless of the individual's status on the sex offender registry in case the individual files a legal claim during the statute of limitations. However, because a records schedule has not been approved, this risk remains unmitigated.

Privacy Risk: Because the AWP receives data from multiple systems/sources, there is a risk that the program collects more information than is necessary.

Mitigation: This risk is mitigated. The ICE Privacy Unit has worked with the AWP to ensure the information the program collects, uses, stores, and discloses about individuals is narrowly tailored to effectively and efficiently carry out the statutorily established purpose of the program. For example, the AWP personnel vet against information maintained in other DHS and U.S. Government records to identify passengers on manifests that are a potential match against NSOR records. In addition, the AWP has technical controls in place to minimize the information disclosed by the AWP to entities outside of DHS. The AWP transmits only the information necessary for USMS to ensure that covered sex offenders are compliant with sex offender registration requirements. This enables the AWP to notify DOS to insert or verify that their passports bear the appropriate covered sex offender marking. Lastly, the notifications sent by the HSI Attaché/CBP liaison office to destination country governments provide only the information needed for an in-country official to identify, to locate the offender, and to assess whether any further action is appropriate.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

The AWP was created to identify U.S. persons convicted of sexual crimes against children who are traveling abroad and, as applicable, notify the destination country's government. This, in turn, reduces the risk of U.S. persons engaging in child sex trafficking and tourism in foreign countries. The notification serves to enable foreign countries to make fully informed decisions relating to the admissibility of U.S. convicted child sex offenders to the foreign country or any other action deemed necessary (e.g., border inspections) without oversharing of PII. Finally, the sharing of information encourages foreign governments to provide the U.S. Government with notifications when foreign nationals convicted of sexual crimes against children travel to the United States.

Privacy Risk: There is a risk that the information will be used by the destination country for purposes beyond those for which the information was shared.

Mitigation: This risk is mitigated. The information shared with the destination country's relevant law enforcement and/or border security officials contains only the information needed to provide situational awareness. In each notification, the HSI Attaché/CBP liaison office will explicitly communicate to the destination country's law enforcement and/or border security officials that AWP is not recommending whether the covered sex offender should be granted entry by the destination country. Any action taken by the destination country as a result of the AWP notification will be in accordance with its laws, regulations, and policy.

The HSI Attaché/CBP liaison office will review the AWP referrals and determine whether the content in the notification intended for the destination country is appropriate (e.g., the destination country government has previously stated a higher minimum threshold should be used before notification is warranted). The HSI Attaché/CBP liaison office will also ensure that AWP contact information is not included in the notification sent to the destination country. This ensures that foreign officials in the receiving country do not try to contact the AWP directly and prevents follow-up requests that are outside the scope of the AWP's purpose.

Lastly, prior to launching in a specific country, each HSI Attaché/CBP liaison office will provide a briefing to the destination country authorities to ensure they understand his or her role with respect to the purpose and scope of the AWP's mission. This includes the creation of protocols with the appropriate law enforcement or border security agency to ensure the destination country's authorities use the information consistent with U.S. law, the destination country's legal authorities, and other binding arrangements (e.g., Customs Mutual Assistance Agreements).

Privacy Risk: There is a risk that data will be shared with agencies external to DHS which do not have a need to know.

Mitigation: This risk is mitigated. Any information shared with third parties is disclosed under the provisions of a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or other data-sharing agreement. ICE shares information with the DOS that identifies information related to the offender's current registration requirements once AWP personnel verify the local sex offender registry requirements. Individuals who receive information from AWP may not further disseminate any data without first obtaining prior approval from ICE and other relevant DHS components. For example, when transmitting travel itinerary, USMS is only authorized to receive current outbound information. Only the HSI Attaché/CBP liaison office may receive a copy of the full itinerary unless USMS officials can demonstrate to AWP personnel a need to know and that the reason is consistent with law and policy. In addition, AWP will verify positive matches to verify that the passenger is the covered sex offender in question. AWP personnel will conduct a manual comparison of the available API with other information maintained in the relevant DOS and DOJ databases, including other publicly available open-source information. Per the MOU for this data exchange, the AWP provides information about covered sex offenders who have a current verified registration requirement in any U.S. jurisdiction. Finally, any information is shared with agencies external to DHS in accordance with the Privacy Act and other applicable law, regulation, and policy.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

AWC personnel vet and review the information obtained from DHS systems and publicly available data sources to ensure accuracy. In addition, the AWP will correct information contained

in the notification made to foreign government agencies or other partner agencies (e.g., USMS, DOS) as appropriate.

Privacy Risk: There is a risk that the source system could contain inaccurate information.

Mitigation: This risk cannot be fully mitigated. However, ICE has taken steps to ensure data quality when vetting records and adequate redress and correction procedures. All possible positive matches are vetted by comparing the API with relevant information available in DOS and DOJ databases, as well as other publicly available open-source information, or by contacting the applicable state or local sex offender registry office. If any data received is inaccurate or there is a discrepancy in information contained in the different sources, AWP personnel can contact the source to request clarification. If the registry office cannot clarify or confirm the accuracy of information associated with an offender, AWP will not send a referral. Lastly, as discussed above, the program has a comprehensive review and redress process that allows U.S. persons to request access to and correction of any inaccurate information about themselves that was disclosed by the program if found to be erroneous. Furthermore, new AWP personnel are prohibited from sending referrals to other agencies until the personnel demonstrate a thorough understanding of how to properly vet passengers, read criminal history, and research relevant criminal statutes.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

Strict physical and technical access controls are in place to ensure the security of all information collected, maintained, and shared by the AWP. Only authorized users whose job duties include executing the AWP mission are granted rights to access the data maintained for AWP purposes. This access is limited to those with a need to know. In the event that PII is been compromised - including misuse of data, unauthorized access, and inappropriate disclosure of Sensitive PII - it will be reported and handled as a privacy incident. For cases in which misconduct is suspected, the incident will be reported to the ICE Office of Professional Responsibility (OPR) for further investigation.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

AWP personnel must have and maintain direct access to ICE's ICM system, which interfaces with the FBI's NCIC database and CBP's system(s). Authorized users take annual privacy, security, and information assurance awareness training before system access is granted. These trainings ensure that users understand the proper handling of PII, as well as relevant security

processes and procedures. Additionally, users must complete system-specific training to certify that they know how the system operates and can properly handle information contained within the system. The AWP also maintains an accounting of disclosures through archived emails that include the AWP personnel who sent each notification, along with the date sent and recipient.

Privacy Risk: There is a risk that unauthorized users may access AWP information.

Mitigation: This risk is mitigated. System administrators employ access controls to ensure that only authorized users can access the data in the system and provide role-based access so that users only have access to the information necessary for his or her position. Certain users may only have "read only" access, while others may have read/write/edit privileges, based on the user's job responsibilities. Individuals who no longer require access have their credentials removed from the system. Also, as mentioned previously, new AWP personnel are prohibited from sending referrals to other agencies until they demonstrate a thorough understanding of how to properly vet passengers, read criminal history, and research relevant criminal statutes.

Contact Official

Alysa D. Erichs
Acting Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Responsible Official

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717