DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Privacy Act of 1974; System of Records Notice

AGENCY: Office on Trafficking in Persons (OTIP), Administration for Children and Families (ACF), Department of Health and Human Services (HHS).

ACTION: Notice of two new systems of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the U.S. Department of Health and Human Services (HHS) is establishing two new systems of records that will be maintained by the Administration for Children and Families (ACF), Office on Trafficking in Persons (OTIP): System No. 09-80-0391, Anti-Trafficking Information Management System (ATIMS) Records; and System No. 09-80-0392, National Human Trafficking Training and Technical Assistance Center (NHTTAC) Participant Records.

DATES: In accordance with 5 U.S.C 552a(e)(4) and (11), this notice of two new systems of records is effective [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The public should address written comments by mail to: Anita Alford, Senior Official for Privacy, Administration for Children and Families, 330 C Street SW, Washington, DC 20201; or by email to: anita.alford@acf.hhs.gov.

FOR FURTHER INFORMATION CONTACT: General questions about the systems of records may be submitted to Beth Kramer, HHS Privacy Act Officer, FOIA/Privacy Act Division, Office of the Assistant Secretary for Public Affairs, U.S. Department of Health and Human Services, by mail at 200 Independence Ave. SW – Suite 729H, Washington, DC 20201, or by telephone at (202) 690-6941, or by email at beth.kramer@hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background on OTIP Functions

On June 10, 2015, the Department of Health and Human Services (HHS), Administration for Children and Families (ACF) established the Office on Trafficking in Persons (OTIP) and delegated to OTIP the authority to administer human trafficking programs formerly administered by ACF's Office of Refugee Resettlement (ORR). In addition to administering human trafficking programs, OTIP provides letters of Certification and Eligibility to foreign national victims of severe forms of trafficking in persons under the authority of the Trafficking Victims Protection Act of 2000, as amended (22 U.S.C. 7105(b)(1), hereafter abbreviated "TVPA"), to enable the victims to apply for federally-funded benefits and services to the same extent as refugees. Under the TVPA, OTIP is authorized to collect data and evaluate the effectiveness and efficiency of programs designed to serve victims of severe forms of trafficking in persons (see 22 U.S.C. 7103(d), 7104(b), 7105(b), and 7105(f)). Through participation on the President's Interagency Task Force to Monitor and Combat Trafficking (PITF), OTIP is authorized to conduct research on the causes, effectiveness, and interrelationship of human trafficking and global health risks while identifying an effective mechanism for quantifying the number of victims of trafficking on a national, regional, and international basis. OTIP authorizations include efforts to:

1. Measure and evaluate progress of the United States in the areas of prevention, protection, and assistance to victims of trafficking;
2. Expand interagency procedures to collect and organize data, including significant research and resource information on domestic and international trafficking with respect to the confidentiality of victims of trafficking; and
3. Engage in consultation and advocacy with government and nongovernmental organizations to advance the purposes of the PITF.

OTIP has determined that its performance of these functions requires maintenance of two new functionally different sets of records that will be subject to the Privacy Act (i.e., records about individuals, retrieved by personal identifier), described in A and B, below. Both sets of records are functionally different from the OTIP consultant records covered in existing HHS departmentwide System of Records Notice (SORN) 09-90-1601, Outside Experts Recruited for Non-FACA Activities.

A. Records to be Covered in New SORN 09-80-0391, Anti-Trafficking Information Management System (ATIMS) Records

SORN 09-80-0391 will cover case files that OTIP maintains about individuals who have or may have been subjected to a severe form of trafficking in persons in accordance with the TVPA. Currently, there are two main file types, briefly described below.

- *Case Files Associated with Requests for Assistance for Foreign National Child Victims of Human Trafficking*

  The TVPA requires federal, state, and local officials to notify HHS not later than 24 hours after discovering that a foreign national minor may be a victim of trafficking (see 22 U.S.C. 7105(b)). OTIP developed a Request for Assistance (RFA) form for requesters (i.e., assistance requesters) to use to notify HHS of trafficking concerns for foreign national minors (non-U.S. citizens or non-lawful permanent residents under

the age of 18) who are currently in the United States and to request assistance on behalf of foreign national minors. Use of this form, or the completion of any section of this form, is optional. When an RFA is received, OTIP creates a case for the individual seeking assistance in an online case management system. OTIP uses case files, which contain information collected through the RFA process, to determine a child's eligibility for interim and long-term assistance (see 22 U.S.C. 7105(b)(1)(G)). If there is sufficient information during the RFA process to indicate that the child was subjected to forced labor and/or commercial sex (i.e., experienced a severe form of trafficking in persons), OTIP will issue an Eligibility Letter, making the child eligible to apply for benefits and services to the same extent as a refugee. If there is sufficient information during the RFA process to indicate that the child may have been subjected to a severe form of trafficking in persons, OTIP will issue an Interim Assistance Letter, making the child eligible to apply for benefits and services to the same extent as a refugee for 90 days, or up to 120 days if extended. During the interim assistance period, OTIP will seek consultation from the U.S. Departments of Justice (DOJ) and Homeland Security (DHS), other government agencies, and nongovernmental organizations (NGOs) before issuing an Eligibility Letter or a Denial Letter. If the information OTIP receives during the RFA process does not indicate that the child may have been subjected to a severe form of trafficking in persons, OTIP will issue a Denial Letter to the child. OTIP will include instructions with the Denial Letter on how to request reconsideration and how to resubmit the child's case, if applicable.

- *Case Files Associated with Requests for HHS Certification of Foreign National Adult Victims of Human Trafficking*

OTIP provides letters of Certification to foreign national adult victims of severe forms of human trafficking under the authority of the TVPA (see 22 U.S.C. 7105(b)(1)). OTIP developed a Request for HHS Certification (RFC) form for requesters (i.e., assistance requesters) to use to provide the required information for foreign national adult victims to obtain a Certification Letter. When an RFC is received, OTIP creates a case for the individual seeking Certification in an online case management system. OTIP uses case files, which contain information collected through the RFC process, to issue a Certification Letter. Certification is required for foreign national adult trafficking victims in the United States to apply for federally-funded benefits and services. Individuals can only receive an HHS Certification Letter if they have received Continued Presence, T-1 Nonimmigrant Status, or a Bona Fide T-1 Visa from the Department of Homeland Security (DHS) that has not been rescinded or denied. These immigration documents may be received and stewarded by OTIP as part of the process to issue a Certification Letter to eligible recipients.

The Privacy Act applies, in its entirety, only to U.S. citizens and lawful permanent residents. The Judicial Redress Act of 2015 (JRA), 5 U.S.C. 552a note, extends the right to pursue certain civil remedies in the Privacy Act (redress rights) to citizens of designated countries. While the above-described files may be about foreign nationals from *any* country, only foreign nationals who are from countries designated in accordance with the JRA have statutory rights under the Privacy Act, which are limited to redress rights.

B. Records to be Covered in New SORN 09-80-0392, National Human Trafficking Training and Technical Assistance Center (NHTTAC) Participant Records

OTIP established the National Human Trafficking Training and Technical Assistance Center (NHTTAC) in 2016, pursuant to authority in the TVPA, to build the capacity of

health and human services professionals and help prevent, identify, and respond to trafficking. OTIP implements the requirements of the Stop, Observe, Ask, and Respond to Health and Wellness Act of 2018 (42 U.S.C. 300d–54) through NHTTAC. NHTTAC works to further the agency's mission by increasing access to user-friendly, efficient, and cost-effective training and technical assistance resources for individuals, organizations, and communities on trafficking-related topics.

SORN 09-80-0392 will cover the following two types of records maintained by NHTTAC in participant files which are retrieved by the participant's name or other personal identifier:

- Records of feedback the individual provides to NHTTAC evaluating NHTTAC training and technical assistance (T/TA) programs and events in which the individual participated, which NHTTAC uses to address or clarify questions or issues raised by the participant; and
- Information about the individual's participation in SOAR *Online* trainings, which is used to issue Continuing Education/Continuing Medical Education (CE/CME) credits earned by participants.

A report on the two new systems of records was sent to OMB and Congress in accordance with 5 U.S.C. 552a(r), by the HHS Senior Agency Official for Privacy (SAOP), or the SAOP's designee, in accordance with OMB Circular A-108, section 7.e.

Dated: April 25, 2024.

Beth Kramer,
HHS Privacy Act Officer,
FOIA-Privacy Act Division,
Office of the Assistant Secretary for Public Affairs.

SYSTEM NAME AND NUMBER:

Anti-Trafficking Information Management System (ATIMS) Records, 09-80-0391.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for the system of records is: Office on Trafficking in Persons (OTIP), Administration for Children and Families (ACF) Immediate Office of the Assistant Secretary (IOAS), Department of Health and Human Services (HHS), Mary E. Switzer Building, 330 C Street SW, Washington, DC 20201.

SYSTEM MANAGER(S) AND ADDRESS(ES):

The agency official who is responsible for the system of records is: System Owner, Office on Trafficking in Persons (OTIP), Administration for Children and Families (ACF) Immediate Office of the Assistant Secretary (IOAS), 330 C Street SW, Washington, DC 20201; Email: EndTrafficking@acf.hhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

22 U.S.C. 7105.

PURPOSE(S) OF THE SYSTEM:

The records in this system of records are used by OTIP to electronically process Requests for Assistance (RFA) and Requests for Certification (RFC), which are submitted to OTIP digitally via an online system that OTIP provides for this purpose and maintained in

electronic case files. The records are accessed by OTIP personnel on a need-to-know basis for these purposes:

1. RFA case files contain information submitted by requesters. These files are used to make prompt determinations regarding a foreign national child's eligibility for assistance, to facilitate the required consultation process should the child receive interim assistance, to connect the child to trafficking-specific, comprehensive case management services through referral, and to assess and address potential child protection issues. OTIP issues an Interim Assistance or Eligibility Letter to a foreign national child in the United States, upon receipt of credible information which substantiates that the child may have been or was subjected to a severe form of trafficking in persons, to enable the minor to apply for federally-funded benefits and services to the same extent as a refugee. Such benefits and services include access to trafficking-specific case management services, medical services, food assistance, cash assistance, health insurance, education, and other needed services.
2. RFC case files contain information submitted by requesters. These files are used to issue a Certification Letter to a foreign national adult trafficking victim to enable the adult victim to apply for federally-funded benefits and services to the same extent as refugees. OTIP issues a Certification Letter to a foreign national adult in the United States who has experienced a severe form of trafficking after OTIP receives notice from the U.S. Department of Homeland Security (DHS) that a Continued Presence, or a T visa, has been granted or that a bona fide T visa application has not been denied with respect to that adult. Benefits and services include access to trafficking-specific case management services, medical services, food assistance, cash assistance, health insurance, education, and other needed services.

3. Records in both types of files may be used to inform HHS research and for quality assurance purposes directed at program improvement and policy development.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records are about the following categories of individuals:

- Foreign national minors identified as potential trafficking victims on RFA forms submitted to OTIP; and
- Foreign national adults identified as trafficking victims on RFC forms submitted to OTIP.

Note: Individuals who submit RFA and RFC forms to OTIP on behalf of trafficking victims or who serve as case management points of contact at other agencies, nongovernmental organizations (NGOs), and other entities that provide benefits and services to trafficking victims are not considered record subjects for purposes of this system of records, because all records involving them are about them in a representative capacity only.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records consist of electronic case files associated with RFAs and RFCs, containing the information described below. The information technology system that OTIP uses to receive RFAs and RFCs and to maintain the case files allows for case file information to be collected through structured fields, open text fields, and document attachments.

- Case files associated with RFAs contain information that is pertinent to an eligibility determination and the case management needs of an individual child. An RFA case file includes: personal identifiers such as the child's name, date of birth, and Alien Registration Number; information about the child's experiences,

including information about the child's background, adverse childhood experiences, and family history; information pertaining to emergency case management or child protection needs, and; information specific to the exploitation the child experienced, including the type of trafficking exploitation experienced, and the industry or venue where that exploitation took place. The case file also contains information about the assistance requester(s) who submitted the RFA on behalf of the child, including their name, phone number, and email address, to facilitate the required consultation process should the child receive interim assistance, to connect the child to trafficking-specific, comprehensive case management services through referral, and to assess and address potential child protection issues.

- Case files associated with RFCs contain information that is pertinent to issuing a Certification Letter to an adult who DHS has identified as having experienced a severe form of trafficking in persons and, to connect the adult to trafficking-specific, comprehensive case management services through referral. The case files include: personal identifiers, such as the adult trafficking victim's name, date of birth, and Alien Registration Number; information pertaining to emergency case management needs; information about the type of trafficking experienced (sex, labor, sex and labor); and related documentation from DHS (Continued Presence, T visa, bona fide T visa documentation and date of issuance). The case files also contain information about the assistance requester(s) who submitted the RFC on behalf of the adult trafficking victim, including their name, phone number, and email address to connect the adult to trafficking-specific, comprehensive case management services through referral, if requested.

RECORD SOURCE CATEGORIES:

Information in case files is provided directly by the trafficking victim or is provided by case managers, attorneys, law enforcement officers, child welfare workers, or other representatives assisting the victim.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974 at 5 U.S.C. 552a(b), under which HHS may disclose information from this system of records without the consent of the data subject. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible and appropriate. For example, information that a Violence Against Women Act (VAWA) funding recipient could not lawfully disclose under the confidentiality provision of that Act, 34 U.S.C. 12291(b)(2), would not be unlawful for HHS to disclose, because HHS is not a VAWA funding recipient so is not subject to that provision; however, it would be inappropriate for HHS to disclose, because HHS chooses to comply with that provision voluntarily.

1. *Disclosure to HHS Contractors, Grant Recipients, and Other Agents.* Information may be disclosed to contractors, consultants, grant recipients, and other agents engaged by HHS to assist in the fulfillment of an HHS function relating to the purposes of this system of records and who need to have access to the records in the performance of their duties or activities for HHS.
2. *Disclosures in Litigation and Other Proceedings.* Information may be disclosed to the Department of Justice (DOJ) or to a court or other adjudicatory body in litigation or other adjudicatory proceedings, when HHS or any of its components, or any employee of HHS in his or her official capacity, or any employee of HHS in her or her individual capacity where

DOJ or HHS has agreed to represent the employee, or the United States Government, is a party to the proceedings or has an interest in the proceedings and, by careful review, HHS determines that the records are both relevant and necessary to the proceedings.

3. *Disclosure to Exchange Information With Other Government Agencies*. Information may be disclosed to the Department of Labor and other government agencies (including foreign, federal, state, Tribal, and local agencies) to exchange information with them for the purpose of preventing and responding to child and adult labor exploitation and trafficking.

4. *Disclosure to Service Provider.* Information may be disclosed to a provider of services to foreign national adults and children, including migrant and refugee youth, a foster care agency or national refugee resettlement agency, or to a local, county, or state institution (e.g., state refugee coordinator, child welfare agency, court, or social service agency) for the purpose of providing trafficking-specific case management services to individuals covered by this system of records.

5. *Disclosure to an Attorney or Representative.* Information may be disclosed to an attorney or representative (as defined in 8 CFR 1.2) who is acting on behalf of an individual covered by this system of records in connection with any proceeding before the Department of Homeland Security or the Executive Office for Immigration Review, or under other circumstances when records are requested by counsel representing individuals covered by this system of records.

6. *Disclosure Incident to Requesting Information.* Information may be disclosed (to the extent necessary to identify the individual, inform the source of the purpose of the request, and identify the type of information requested), to any

source from which additional information is requested when necessary to obtain information relevant to an agency decision concerning benefits.

7. *Disclosure to Congressional Office.* Information may be disclosed to a congressional office from the record of an individual in response to a written inquiry from the congressional office made at the written request of the individual.

8. *Disclosure in Connection with Settlement Discussions.* Information may be disclosed in connection with settlement discussions regarding claims by or against HHS, including public filing with a court, to the extent that disclosure of the information is relevant and necessary to the discussions.

9. *Disclosure for Monitoring Waste, Fraud, or Abuse Purposes.* Information may be disclosed to another Federal agency or instrumentality of any governmental jurisdiction within or under the control of the United States (including the State or local governmental agency) that administers or has the authority to investigate potential fraud, waste, or abuse in federally-funded programs, when disclosure is deemed reasonably necessary by HHS to prevent, deter, discover, detect, investigate, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.

10. *Disclosure in the Event of a Security Breach Experienced by HHS.* Information may be disclosed to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records; (2) HHS has determined, as a result of the suspected or confirmed breach, there is a risk of harm to individuals, the agency (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 HHS' efforts to respond to the suspected or confirmed breach, or to prevent, minimize, or remedy such harm.

11. *Disclosure to Assist Another Agency Experiencing a Breach.* Information may be disclosed to another federal agency or federal entity, when HHS 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The records are stored electronically, in a database which is backed-up on a daily basis.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Each individual who is identified in an RFA or RFC as a trafficking victim or potential victim is assigned a unique case identification number (i.e. HHS Tracking Number). OTIP (and assistance requesters who submit RFAs and RFCs to OTIP) retrieves records by the trafficking victim's name (first, middle, last), date of birth, and Alien Registration Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A disposition schedule is currently pending approval by the National Archives and Records Administration (NARA). When approved by NARA, it will provide for case file

information gathered during the RFA and RFC processes, in identifiable form, to remain in HHS' custody for 15 years, or longer if needed for HHS' business use. Under a separate, NARA-approved disposition schedule, DAA-0292-2020-0001, the records that have met their retention period under the pending schedule will be accessioned (in identifiable form, in case needed for investigative purposes) to the National Archives of the United States for permanent retention.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Safeguards conform to the HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html. Information is safeguarded in accordance with applicable laws, rules and policies, including the HHS Information Systems Security and Privacy Policy (IS2P), all pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A-130 Managing Information as a Strategic Resource. Records will be protected from unauthorized access through appropriate administrative, technical, and physical safeguards under the supervision of the ACF Office of the Chief Information Security Officer (OCIO). The system leverages cloud service providers that maintain an authority to operate in accordance with applicable laws, rules, and policies, including Federal Risk and Authorization Management Program (FedRamp) requirements.

Administrative safeguards include requiring security and privacy training for Federal personnel and contractor staff and requiring Rules of Behavior (ROB) to be signed by database users. Technical controls include role-based access, user identification, passwords, firewall, and maintenance of intrusion detection functionality. Physical controls include the use of nondescript facilities to house the database and backup equipment, with security staff controlling both the perimeter and various ingress points within the buildings, video surveillance, intrusion detection systems, fire detection and

suppression, uninterruptible power supply (UPS), and climate control. Additionally, all individuals accessing the buildings are required to use two-factor authentication a minimum of two times for entry, and any visitor or contractor must sign in and be escorted at all times by an authorized individual.

RECORD ACCESS PROCEDURES:

An assistance requester may check the status of an RFA or RFC the assistance requester submitted on behalf of a victim (subject individual) via the online verification page, https://shepherd.otip.acf.hhs.gov/shepherdpublic/letterverification, using the HHS Tracking Number and one of the following: victim's date of birth, last name, or benefits start date.

All other requests for information about a victim referred to OTIP through a RFA or RFC must be made in writing by the subject individual's legal representative on the law firm or legal agency's letterhead. The request must be sent to the email address (EndTrafficking@acf.hhs.gov) or mailing address specified in the "System Manager(s)" section of this SORN. The request letter must include: the name, alias, date of birth, nationality, and Alien Registration Number of the subject individual, the name of the requesting legal representative, and the reasons why the records are being requested. The following supporting documentation must also be submitted:

- A copy of the signed and executed *G-28, EOIR-27* or *EOIR-28*. These forms are not required for attorneys who work for, or volunteer pro bono services for, non-profit legal service providers funded by the VERA Institute of Justice for ORR's Division of Children's Services' legal access and outreach project
- An *Authorization for Release of Confidential Records* on the law firm/legal agency's letterhead stationery signed by the subject individual if the subject

individual is 14 years of age or older and is not legally incompetent or by the subject individual' parent or legal guardian if the subject individual is under 14 years of age or is legally incompetent.

- The authorization must specify to whom the requested records should be released and the duration of the authorization.

So that OTIP may verify the identities of the subject individual and the subject individual's requesting legal representative (and, if applicable, the subject individual's parent or legal guardian), their signatures must be notarized or the request must include, for each of them, a written, signed certification signed under penalty of perjury stating that he/she is the individual who he/she claims to be and that he/she understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000. Evidence of any parent or guardian relationship must also be provided with the request, unless previously provided to OTIP.

CONTESTING RECORD PROCEDURES:

Individuals seeking to amend records about them in this system of records must submit a written amendment request to the System Manager identified in the "System Manager(s)" section of this SORN, containing the same information required for an access request. The amendment request must include verification of identities in the same manner required for an access request; must reasonably identify the record and specify the information contested, the corrective action sought, and the reasons for requesting the correction; and should include supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

NOTIFICATION PROCEDURE:

Individuals who wish to know if this system of records contains records about them must submit a written notification request to the System Manager identified in the "System Manager(s)" section of this SORN. The notification request must contain the same information required for an access request and must include verification of identities in the same manner required for an access request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

SYSTEM NAME AND NUMBER:

National Human Trafficking Training and Technical Assistance Center (NHTTAC) Participant Records, 09-80-0392.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for the system of records is: Office on Trafficking in Persons (OTIP), Administration for Children and Families (ACF) Immediate Office of the Assistant Secretary (IOAS), Department of Health and Human Services (HHS), Mary E. Switzer Building, 330 C Street SW, Washington, DC 20201.

SYSTEM MANAGER(S) AND ADDRESS(ES):

The agency official who is responsible for the system of records is: System Owner, Office on Trafficking in Persons (OTIP), Administration for Children and Families (ACF) Immediate Office of the Assistant Secretary (IOAS), 330 C Street SW, Washington, DC 20201; Email: EndTrafficking@acf.hhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

22 U.S.C. 7105, 42 U.S.C. 300d-54.

PURPOSE(S) OF THE SYSTEM:

OTIP established the National Human Trafficking Training and Technical Assistance Center (NHTTAC) to build the capacity of health and human services professionals and help prevent, identify, and respond to trafficking through training and technical assistance

(T/TA). On OTIP's behalf, NHTTAC collects personally identifiable information (PII) about participants in NHTTAC's T/TA offerings to inform evaluation efforts, to assess customer satisfaction with T/TA offerings, and to issue Continuing Education/Continuing Medical Education (CE/CME) credits to eligible participants. Within NHTTAC, identifiable records about participants are retrieved by personal identifier and used by NHTTAC personnel on a need-to-know basis, for these purposes:

- To identify individuals who submit applications and their needs for specialized and/or short-term training and technical assistance from OTIP, including geographic locations where T/TA is requested and provided.
- To identify individuals who enroll in and complete the Stop. Observe. Act. Respond. (S.O.A.R) Health and Wellness online (SOAR *Online)* and in-person training program and receive CE/CME credits for their participation.
- To report the fulfillment of Continuing Education/Continuing Medical Education (CE/CME) credits to the appropriate accrediting bodies.

On a need-to-know basis, information from this system of records may be shared with relevant offices within HHS, including OTIP. OTIP and the following offices support NHTTAC activities, particularly through the SOAR Coordinating Group, and might receive participant contact information (e.g., name, email address and/or phone number) once OTIP has approved the delivery T/TA services and for future T/TA planning purposes: Office of the Chief Information Officer (OCIO), Substance Abuse and Mental Health Services Administration (SAMHSA) Center for Substance Abuse Treatment (CSAT), Health Resources and Services Administration (HRSA) Office for Women's Health (OWH), Office of the Assistant Secretary for Health (OASH) Office on Women's Health (OWH), Center for Disease Prevention and Control (CDC) Division of Violence Prevention (DVP), and OASH Office of Regional Operations (ORO). The PII is provided through the NHTTAC interface, encrypted email message, or by phone.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records are about multidisciplinary anti-trafficking professionals, such as health care professionals, child welfare professionals, and other service providers, who participate in NHTTAC T/TA offerings.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records consist of participant files. The information technology system that NHTTAC uses to maintain the files allows for participant file information to be collected through structured fields, open text fields, and document attachments. Files include identifiable information about participants, including their name (first, last), mailing address, email, and phone number, and may also include information about certificates received (e.g. training completion confirmations), and self-reported demographic information such as race/ethnicity, date of birth, gender identity, employment status, education history, employment history, professional history, language proficiency, user login name and password (user credentials), responses to requests for feedback on NHTTAC T/TA offerings, and T/TA needs assessment responses submitted on behalf of the participant or the participant's professional organization.

RECORD SOURCE CATEGORIES:

Most records are provided directly by the NHTTAC T/TA participant. Continuing education credits are issued by NHTTAC based on records in the online system confirming that the individual completed SOAR *Online* trainings. T/TA needs assessment responses may be provided by the individual participant, or representatives of the participant's professional organization.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to the disclosures authorized by statute in the Privacy Act at 5 U.S.C. 552a(b), HHS may disclose records about an individual participant from this system of records for these routine uses:

1. *Disclosure to HHS Contractors, Grant Recipients, and Other Agents.* Information may disclosed to contractors, consultants, grant recipients, or other agents engaged by HHS to assist in the accomplishment of an HHS function relating to the purposes of this system of records who need to have access to the records in the performance of their duties or activities for HHS.
2. *Disclosure to Accrediting Bodies.* Information about a SOAR *Online* participant's fulfillment of Continuing Education/Continuing Medical Education (CE/CME) credits may be reported to the appropriate accrediting bodies.
3. *Disclosure to Congressional Office.* Information may be disclosed to a congressional office from the record of an individual in response to a written inquiry from the congressional office made at the written request of the individual.
4. *Disclosure for Monitoring Waste, Fraud, or Abuse Purposes.* Information may be disclosed to another Federal agency or instrumentality of any governmental jurisdiction within or under the control of the United States (including the State or local governmental agency) that administers or has the authority to investigate potential fraud, waste, or abuse in federally-funded programs, when disclosure is deemed reasonably necessary by HHS to prevent, deter, discover, detect, investigate, sue with respect to defend

against, correct, remedy, or otherwise combat fraud, waste or abuse in such programs.

5. *Disclosure in the Event of a Security Breach Experienced by HHS.* Information may be disclosed to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records; (2) HHS has determined, as a result of the suspected or confirmed breach, there is a risk of harm to individuals, the agency (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 HHS' efforts to respond to the suspected or confirmed breach, or to prevent, minimize, or remedy such harm.

6. *Disclosure to Assist Another Agency Experiencing a Breach.* Information may be disclosed to another federal agency or federal entity, when HHS 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in electronic media format, in a web-based application. Feedback records may be maintained in paper form before being entered in the web-based system.

POLICIES AND PRACTICIES FOR RETRIEVAL OF RECORDS:

NHTTAC retrieves records about a participant by the participant's name (first, last), address, phone number, and email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records are currently unscheduled. Unscheduled records must be retained indefinitely pending the agency's submission, and the National Archives and Records Administration (NARA) approval, of a disposition schedule. OTIP is currently coordinating with the HHS Office of the Chief Information Officer (OCIO) to develop a Records Control Schedule (RCS) appropriate for these records. OTIP currently plans to propose a retention period of approximately 10 years for the records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Information is safeguarded in accordance with applicable laws, rules and policies, including the HHS Information Systems Security and Privacy Policy (IS2P), all pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A-130 Managing Information as a Strategic Resource. The system leverages cloud service providers that maintain an authority to operate in accordance with applicable laws, rules, and policies, including Federal Risk and Authorization Management Program (FedRAMP) requirements.

The NHTTAC system will be hosted within the FedRAMP Amazon Web Services (AWS) Cloud Platform. Only members of the NHTTAC team are granted access to the web-based system and to any feedback records that are in paper form. Any paper feedback records are maintained in a locked filing cabinet with limited access until entered into the web-based system. Authenticated users within the system have access to review and edit their own PII. Authenticated users in roles with elevated permissions will

have access to larger amounts of PII that is specific to certain system purposes. The elevated privilege accounts are associated with specific system features and are granted only to federal OTIP staff or the NHTTAC contractors. The administrator account, Admin Only, is limited to administrative activity only and does not allow for other activity within the application. This role is held by NHTTAC contractors and OCIO personnel. Administrators will have access to PII to support system setup, configuration, testing, monitoring, and other data/system administration. The administrative security controls employed include adhering to ACF, or HHS, policies and procedures around security and privacy; leveraging role-based system access to control the amount of PII available to a user; annual security training, and access to a user manual describing data entry procedures to help maintain the data integrity. The technical controls are shared between the system and the AWS platform. The system provides controls including multi-factor authentication for all users to include Personal Identity Verification (PIV) login capability; and AWS provides infrastructure controls including secure network access points. PII is encrypted at rest within the database, file system, and object storage resources using Advanced Encryption Standard algorithm in Galois/Counter Mode (AES-GCM), with 256-bit secret keys. PII is also encrypted in transit via secure hypertext transfer protocol (HTTPS) using Transport Layer Security (TLS) services provided by Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules. The physical controls will all be inherited by the AWS platform and include the following: Restricting physical access to the data center both at the perimeter and at building ingress points through the help of video surveillance, intrusion detection systems, and 2 rounds of two-factor authentication for each individual accessing a data center floor. Visitors and contractors are required to have ID, sign-in with building security, and be escorted by an authorized staff at all times; Fire detection and suppression systems; Uninterruptible Power Supply (UPS); Climate and Temperature

control; Preventative maintenance. Staff are responsible for notifying the ACF Incident Response Team (IRT) in the event that a suspected or known breach has occurred. The ACF IRT will follow standard operating procedures for handling a privacy incident that involves a breach of PII.

RECORD ACCESS PROCEDURES:

Participants who are authenticated users of the web-based system have the ability to access information about them in that system. Otherwise, participants seeking access to records about them in this system of records must submit a written access request to the relevant System Manager identified in the "System Manager(s)" section of this SORN. The request must contain the requester's (participant's) full name, address, telephone number and/or email address, date of birth, and signature, and should identify the state, Tribe, or territory where the requester participated in the NHTTAC T/TA offering.

So that HHS may verify the requester's identity, the requester's signature must be notarized, or the request must include the requester's written, signed certification that the requester is the individual who the requester claims to be and that the requester understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000.

CONTESTING RECORD PROCEDURES:

Participants who are authenticated users of the web-based system have the ability to amend identifying and descriptive information about them in the system, which they entered in the system. Otherwise, participants seeking to amend records about them in this system of records must submit a written amendment request to the relevant System Manager identified in the "System Manager(s)" section of this SORN, containing the

same information required for an access request. The request must include verification of the requester's (participant's) identity in the same manner required for an access request; must reasonably identify the record and specify the information contested, the corrective action sought, and the reasons for requesting the correction; and should include supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

NHTTAC provides support for individuals who indicate concerns that information about them has be inappropriately obtained, used, or disclosed, or is inaccurate. To support initial reporting of concerns, the web-based system includes contact information for NHTTAC support staff on the home page. Once contacted, NHTTAC will establish an issue/ticket associated with the concern, and track progress towards issue resolution within a separate internal help desk system monitored by the NHTTAC support staff. The participant will be contacted via his or her provided contact information (email or phone) upon initiation of the ticket, as progress is made, and upon resolution of the issue.

NOTIFICATION PROCEDURE:

Participants who are authenticated users of the web-based system have the ability to access the system to determine if it contains records about them. Otherwise, participants who wish to know if this system of records contains records about them should submit a written notification request to the relevant System Manager identified in the "System Manager(s)" section of this SORN. The request must contain the same information required for an access request and must include verification of the requester's (participant's) identity in the same manner required for an access request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2024-09343 Filed: 5/1/2024 8:45 am; Publication Date: 5/2/2024]