Privacy Impact Assessment

for the

Alternatives to Detention (ATD) Program

DHS Reference No. DHS/ICE/PIA-062

March 17, 2023

Homeland Security

Abstract

U.S. Immigration and Customs Enforcement (ICE) Office of Enforcement and Removal Operations (ERO) oversees and manages Alternatives to Detention (ATD) programs, including the Young Adult Case Management Program (YACMP) and the primary Alternatives to Detention program, the Intensive Supervision Appearance Program (ISAP) (hereinafter collectively referred to as "ICE ATD programs"). ICE ATD programs consist of two parts: the oversight of case management support services and compliance with ICE immigration reporting requirements set forth by ICE. ICE ATD programs allow eligible noncitizens age eighteen (18) and older in immigration proceedings who are not detained in an immigration facility to remain in their selected community pending the outcome of their immigration case. The Office of Enforcement and Removal Operations has sole and complete oversight over both ICE ATD programs, specifically, the assignment and supervision of case management services offered under these programs, along with supervising electronic monitoring and/or reporting requirements. The combination of Enforcement and Removal Operations supervision of case management services and use of electronic monitoring or other monitoring and reporting requirements ensures compliance with immigration requirements and increases the rate of court appearances. In accordance with ICE's legal authorities and mission, Enforcement and Removal Operations personnel enforce supervision and reporting requirements upon all ATD participants, including those whose case management services are overseen and managed by the Department of Homeland Security (DHS) Office of Office Civil Rights and Civil Liberties (CRCL) through the Case Management Pilot Program (CMPP).[1] This Privacy Impact Assessment describes how ICE ATD programs operate in a manner that includes privacy and civil liberties safeguards in accordance with law, regulation, and policy.

Overview

The ICE Office of Enforcement and Removal Operations manages the nation's civil immigration detention system. Noncitizens who are apprehended and determined to need custodial supervision are placed in detention facilities. Noncitizens whose lawful presence in the United States cannot be established and are not sent to ICE detention facilities are placed on the non-detained docket.[2] Every case, whether detained or non-detained, remains part of Enforcement and

[1] CMPP is an ATD program that operates under the DHS Office of Civil Rights and Civil Liberties (CRCL). For more information regarding CMPP, including how it is managed and overseen by a National Board chaired by the DHS CRCL Officer, and the privacy risks and description of mitigation measures, please see Appendix A to this Privacy Impact Assessment. Pursuant to the 2021 Department of Homeland Security Appropriations Act candidates enrolled in ICE ATD programs are eligible for CMPP. While case management services for CMPP participants are overseen and provided entirely through CMPP, as with all noncitizens on the non-detained docket (see footnote 2), participants' immigration cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements.

[2] The U.S. Department of Justice (DOJ) Executive Office for Immigration Review (EOIR) "detained docket" is a court docket that consists of cases involving noncitizens in ICE custody at detention facilities, service processing

Removal Operations' caseload and is actively managed until it is formally closed. Enforcement and Removal Operations processes and monitors detained and non-detained cases as noncitizens move through immigration court proceedings to conclusion.

ICE ATD programs provide a cost-effective alternative to detention for a subset of noncitizens who are deemed suitable for enrollment on ICE's non-detained docket. ICE ATD programs are flight-mitigation programs that use case management tools in combination with electronic monitoring or other monitoring (e.g., criminal background checks) and program reporting requirements to assist enrolled noncitizens' compliance with release conditions, such as attendance at court hearings and compliance with final orders of removal that the U.S. Department of Justice (DOJ) Executive Office for Immigration Review (EOIR) may issue. ICE ATD programs may be appropriate for noncitizens on the non-detained docket who are released pursuant to an Order of Release on Recognizance,[3] Order of Supervision,[4] grant of parole,[5] or bond[6] (unless the custody determination does not allow for participation in ATD).

ATD is not a form of custody; rather, it is a program that provides for supervision over some noncitizens on the non-detained docket using case management services and, as appropriate, monitoring technologies. The goal of ICE ATD programs is to reduce friction with the immigration process and provide and/or facilitate referrals and access to services in the community so that participants remain compliant and engage with the immigration system and process. ICE ATD programs, YACMP and ISAP, provide contractor-facilitated (i.e., ATD Servicer)[7] community-based services tailored to individual participant needs and serve as a central means to monitor

centers, or incarcerated noncitizen inmates in the custody of departments of corrections. The "non-detained docket" is a court docket that consists of cases involving noncitizens not being held in an ICE detention facility.

[3] An Order of Recognizance releases an individual from ICE custody with reporting conditions while in removal proceedings and awaiting a final decision.

[4] An Order of Supervision allows ICE to place conditions on and monitor noncitizens with final orders of removal who have been temporarily released from DHS custody in advance or their removal due to a variety of circumstances. Orders of Supervision contain conditions for release, including but not limited to, a requirement that noncitizens cooperate with efforts to procure travel documents for removal, report to DHS on designated dates, and present themselves for removal once arranged.

[5] Parole is the discretionary authority to allow a noncitizen temporary entry into the United States on a case-by-case basis for urgent humanitarian reasons or significant public benefit. Parole is an extraordinary measure and not intended to be used to avoid normal visa processing procedures and timelines, to bypass inadmissibility waiver processing, or to replace established refugee processing channels.

[6] The immigration bond program allows ICE to release from ICE custody on bond certain noncitizens who have been placed in removal proceedings before an immigration judge. The bond itself is a legally binding written contract between DHS and an obligor (an individual, entity, or surety company) and is posted as security for performance and fulfillment of the bonded noncitizen's obligations to DHS. Immigration bonds may be posted for the release from detention of noncitizens in removal proceedings and/or as voluntary departure bonds.

[7] For the purposes of this Privacy Impact Assessment, contractor-facilitated case management services are provided by a "federal contractor" or "contractor," which is an entity contracted to operate aspects of an ICE ATD program on behalf of and under the oversight of ICE Enforcement and Removal Operations. A contractor may provide materials, personnel, and/or services and are required to adhere to the same laws, regulations, and policies as ICE employees.

participants and to promote compliance with their immigration obligations. In some cases, case management services will be provided directly by Enforcement and Removal Operations program personnel at ICE field offices that maintain the resources required to manage ICE ATD participants. Enforcement and Removal Operations officers and the ATD Servicer's personnel may be referred to collectively as "ATD Case Managers" or "program personnel"[8] for purposes of this Privacy Impact Assessment.

ICE ATD program participants are enrolled in an ICE ATD case management system and ICE's Enforce Alien Removal Module within the Enforcement Integrated Database.[9] ATD participants in ISAP are tracked in the ISAP ATD case management system, which leverages the use of electronic monitoring technology.[10] Whereas, ATD YACMP participants' information is maintained in the YACMP ATD case management system and electronic monitoring technology is not used.[11] As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements set forth under the non-detained docket management process, such as conducting criminal background checks. Once an ATD program candidate (discussed in more detail below) is determined to be suitable for participation in an ICE ATD program, the ICE ATD Case Manager will update the Custody Actions and Decisions tab in the Enforce Alien Removal Module to show

[8] In some cases, the roles of Enforcement and Removal Operations officer and contractor ICE ATD Case Managers may differ. For example, only Enforcement and Removal Operations officers serving as ICE ATD Case Managers can refer participants for prosecution or take enforcement actions. In situations where it is necessary to involve Enforcement and Removal Operations officers, an ICE ATD Servicer must refer the case to an Enforcement Removal and Operations officer ICE ATD Case Manager. However, most of the functions of all ICE ATD Case Managers are consistent enough that, except when otherwise noted, the term will encompass both Enforcement and Removal Operations officer and contractor ICE ATD Case Managers.

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND IMMIGRATION ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), RISK ASSESSMENT CLASSIFICATION ASSESSMENT (RCA 1.0), ENFORCE ALIEN REMOVAL MODULE (EARM 5.0), AND CRIME ENTRY SCREEN (CES 2.0), DHS/ICE/PIA-015(d) (April 6, 2012), *available at* https://www.dhs.gov/privacy-documents-ice.

[10] The ISAP ATD program's current case management system is the Intensive Appearance Technology Services Systems (IATSS) (hereinafter "ISAP ATD case management system"), which maintains all ICE ATD participant information and the capability to monitor ISAP ATD participants in the ICE ISAP ATD program. The ISAP case management system provides a holistic case management system for the ICE ATD program, as well as electronic monitoring capabilities, as needed, allowing ICE ATD Case Managers to efficiently and securely monitor, measure, and report the case management status (e.g., court cases, check-in appointments, face-to-face visits with case managers) of program participants. In addition, the ICE ISAP ATD case management system allows the ICE ATD Servicer to track, monitor, and notify ICE of any significant developments in an individual's case, including when individuals fail to appear for their scheduled court hearings or other appointment as required by their conditions of release.

[11] The YACMP ATD program's current case management system is the Young Adult Resource Data System (YARDS) (hereinafter "YACMP ATD case management system"), which maintains all YACMP ATD participant information and the capability to monitor ICE ATD participants enrolled in the ICE YACMP ATD program. In addition, the YACMP ATD case management system allows the ICE ATD Servicer to monitor and notify ICE of any significant developments in an individual's case, including when individuals fail to appear for their scheduled court hearings or other appointment as required by their conditions of release.

in which ICE ATD program the candidate is enrolled.[12]

ATD Program Violations

For YACMP and ISAP, ICE ATD Case Managers and participants remain in touch throughout the ICE ATD process. Participants may submit a written request for reconsideration of the reporting or monitoring requirements. Requests must include justification for why reconsideration is appropriate along with relevant documentation, if any, to support the request. If a participant does not comply with conditions of release or ICE ATD program rules, the ICE ATD Case Manager can consider:

- Issuing a written warning to the participant and documenting the warning in the Enforce Alien Removal Module;
- Modifying the participant's reporting frequency;
- Changing the type of monitoring/verification technology assigned to the participant; or
- Modifying release conditions.

As noted above, Enforcement and Removal Operations does not oversee and manage the case management services provided under the DHS CRCL ATD program, CMPP. However, as with all noncitizens on the non-detained docket, CMPP participants' immigration cases remain under ICE supervision and participants are required to adhere to ICE reporting and check-in requirements, which are tracked in ICE's Enforce Alien Removal Module. CMPP staff explain to CMPP participants their immigration compliance and ICE check-in requirements, as well as other conditions of release, such as the CMPP participant's responsibility to provide and update Enforcement and Removal Operations with accurate information (e.g., change of address).[13]

ATD Program Absconders

As with all noncitizens on the non-detained docket, an ATD absconder is an ATD participant who, while enrolled in any ATD program, cannot be located, such as when an ATD participant fails to appear at their court hearing. An absconder can be pre-order, post-order, in the appeals process of removal proceedings or pending issuance of a Notice to Appear. Whether the ATD participant is deemed to be an absconder is determined on a case-by-case basis and after all attempts to locate them are exhausted. Once an ATD participant is assessed to be an absconder, they will be removed from the program. Re-enrollment in the program may be possible depending on the facts of the case in question.

[12] For the YACMP ICE ATD program, all information is currently stored in the YACMP ATD case management system (discussed in more detail below). Forthcoming changes to the YACMP ATD case management system will allow information to be shared and stored in ICE's Enforce Alien Removal Module.
[13] For more information, see the CMPP Appendix to this Privacy Impact Assessment.

For ISAP, the ICE ATD Case Manager may attempt to locate the global positioning system unit, if applicable, call individuals on the participant's contact list,[14] run searches of employment history and use any other legally-permissible means to assist in locating the participant—such as visits to any last known ICE ATD participant addresses—to complete a thorough investigation into the absconder's whereabouts. If an absconder is located, ICE ATD Case Managers, who are also ICE law enforcement officers, weigh the totality of the circumstances to determine if the individual is subject to arrest, detention, removal, or re-enrollment in an ICE ATD program.

Prosecution for Failure to Comply

If an ATD participant willfully fails to depart when ordered to do so, or fails to comply with the conditions of release, Enforcement and Removal Operations may refer the participant to DOJ for prosecution under 8 U.S.C. § 1253(a) (failure to depart) or § 1253(b) (willful failure to comply with terms of release under supervision). Under YACMP and ISAP, ICE ATD Servicer personnel (i.e., federal contractors) do not make such determinations, rather ICE ATD Servicer must refer relevant cases to Enforcement and Removal Operations personnel for assessment. Penalties for failure to depart under section 1253(a) include a fine under Title 18, or imprisonment for not more than four years. Penalties for willful failure to comply under section 1253(b) include a fine of not more than $1,000, imprisonment for not more than one year, or both.

Termination from the ICE ATD Program

If Enforcement and Removal Operations determines that a participant should no longer participate in either the YACMP or ISAP programs, the ICE ATD Servicer is provided with Form 71-018, *Notice to Terminate ATD Participation*. The ICE ATD Servicer and Enforcement and Removal Operations program personnel will terminate the participant from ICE ATD participation and Enforcement and Removal Operations will remove the former participant from the ICE ATD program by updating the Custody Actions and Decisions tab in the Enforce Alien Removal Module case file to show that the candidate is no longer a participant enrolled in the ICE ATD program.

ICE ATD Program – Young Adult Case Management Program

YACMP is a new ICE ATD program that is overseen and managed by the ICE Office of Enforcement and Removal Operations Juvenile and Family Management Division. YACMP is being established beginning in 2023 at sixteen locations in the United States— Boston, Chicago, Dallas, Denver, Detroit, El Paso, Houston, Los Angeles, Miami, New York, Orlando, Philadelphia, Phoenix, San Antonio, San Diego, and Washington, DC/Baltimore.

YACMP provides case management services and appropriate monitoring services for participating non-dangerous, low flight-risk young adults within a framework that promotes

[14] The participant contact list is collected when the participant is placed in an ICE ATD program. The contact list includes individuals to be contacted if a participant fails to check in with the program or cannot be located using their global positioning system monitoring device or other electronic monitoring.

compliance with immigration obligations until removal or other resolution of their cases. There is a separate program for young adults because they may not know when they are required to appear in court, understand their legal rights and obligations, and may not be aware of possible community services available to them. Further, they are vulnerable to trafficking when there is no continued verification or confirmation of their safety.

YACMP does not include global positioning system or other electronic monitoring technology. Through a network of community and nongovernmental organizations, YACMP provides services such as legal orientation programs, referrals to legal service providers, communications with ICE or Executive Office of Immigration Review for court dates and ICE reporting, human trafficking screenings, consulate communications, referrals to social service providers, and repatriation services. Eligibility for these services, as well as a participant's conditions of release, are determined based on an individualized service plan and assessment, which is issued for every YACMP participant.

Eligibility for YACMP

YACMP is designed to assist young adults—ages 18 to 19—who age out of the Department of Health and Human Services (HHS), Office of Refugee Resettlement custody, are released from custody, or who are currently reporting to ICE's non-detained docket. YACMP aims to promote compliance with participants' release conditions, including any required reporting to ICE Enforcement and Removal Operations, immigration court hearings, and final orders of removal, while allowing participants to remain in the community and maintain access to community services for the duration of the immigration process without the use of electronic monitoring (i.e., global positioning or monitoring phone application devices). As noted above, this population of young adults may not know when they are required to appear in court, understand their legal rights and obligations, and may not be aware of possible community services available to them.

YACMP ATD Enrollment Process and Reporting Requirements

YACMP participant referrals are received via email. Enforcement and Removal Operations receives referrals in three ways:

- The individual (age 18-19) reports to an ICE Field Office and is referred to YACMP in their jurisdiction;
- ICE Field Office Juvenile coordinators working with the HHS Office of Refugee Resettlement refer the individual in Office of Refugee Resettlement custody, when the individual turns 18 (i.e., ages out" of the HHS Office of Refugee Resettlement program); or
- ICE runs a report of the ICE non-detained docket and refers eligible individuals to YACMP.

The referring entity must provide the following information when refereeing a participant into the program: name, date of birth, and A-Number. Once referred, the individual will receive a YACMP Participant Flyer with instructions to call the appropriate ICE program to make an appointment and report to one of the sixteen program locations (identified above) by a specific date.

The ATD Case Manager will create a new profile in the YACMP ATD case management system with the referral information obtained, as well as name, phone number, and email address of the referral source. During the check-in meeting with ICE, the ATD participant will undergo the orientation process, which informs the ATD participant of the program rules and ICE ATD's reporting and check-in requirements. In addition, the ICE Case Manager will review the YACMP Individual Service Plan with the ATD participant, and complete the "Young Adult Assessment" form. The ATD participant must sign the "YACMP Program Orientation Attestation" form acknowledging that they have undergone the orientation process and understand the program rules and reporting check-in requirements.

YACMP does not use electronic monitoring technology, such as a global positioning system device or a Monitoring App. As with all noncitizens on the non-detained docket, YACMP participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements set forth under the non-detained docket management process, such as conducting criminal background checks.

YACMP Information Collection for Enrollment

In addition to confirming the information provided by the referring entity, additional information is collected from the YACMP participant to be used for their YACMP Individual Service Plan and Young Adult Assessment forms (hereinafter "YACMP-related forms"):

- Full name;
- Date of birth;
- contact information (e.g., phone number, email address), including address of residence and proof of residence documentation, A-Number, medical information (e.g., mental health records, vaccinations), high school records and dependent names and school addresses (if applicable);
- Court records— court name, address, and court dates;
- Immigration Status, indication of suspicion of human trafficking; and
- Community resource needs and referral information—community organization name, address, and contact information for other service referrals (e.g., transportation).

As noted above, the case manager will create a new profile in the YACMP ATD case management system and update the YACMP participant's case file with the additional information collected

during enrollment. Additionally, the case manager is required to complete a human trafficking screening on every individual when they turn 18, using an ICE-approved trafficking assessment tool, the Trafficking Victim Identification Tool (TVIT[15]). Information gathered from the assessment (i.e., whether they are a confirmed victim of or at risk for human trafficking) will be entered into the YACMP ATD case management system by the ATD Case Manager.

ICE will remove an enrollee from the program if the YACMP participant has moved out of one of the sixteen program areas (identified above), the individual is noncompliant with the program, the individual turns twenty years old, or the individual no longer has a pending immigration case.

ICE ATD Program – Intensive Supervision Appearance Program (ISAP)

ISAP is overseen and managed by the ICE Office of Enforcement and Removal Operations Non-Detained Division. This program consists of a combination of case management services and the use of technology tools (e.g., global positioning system) to ensure compliance with the ICE ATD program and conditions of release. As noted above, contractor-facilitated case management services are overseen by ICE Enforcement and Removal Operations or by Enforcement and Removal Operations' field office.

Eligibility for the ISAP ATD Program

ICE ATD Case Managers accept potential candidates primarily through referrals—also referred to as a referral source—which may come from other DHS components, such as U.S. Customs and Border Protection (CBP) or U.S. Citizenship and Immigration Services (USCIS); other ICE offices, such as Homeland Security Investigations (HSI); and other federal, state, and local law enforcement agencies. These entities do not make ICE ATD program eligibility determinations, only referrals. The referring agency or department is documented in ICE systems and informs ICE which agency or department initially encountered the noncitizen. Absent extraordinary circumstances, noncitizens 18 years of age or older may be eligible for placement into the ICE ATD program if they are in removal proceedings and the ICE ATD program is not prohibited by court order. Individual candidates are evaluated on a case-by-case basis before they are placed in the program. Enforcement and Removal Operations personnel consider a number of factors, such as age, medical status, and criminal history, when assessing if ICE ATD program enrollment is appropriate.

ISAP ATD Enrollment Process

Upon the noncitizen's arrival to the United States and suitability for enrollment determinations by Enforcement and Removal Operations, the ICE ATD Case Manager verifies the

[15] The Traffic Victim Identification Tool is an ICE-approved tool created by the VERA Institute; an independent nonprofit entity supported by the National Institute of Justice. For more information, please see A Screening Tool for Identifying Trafficking Victims | National Institute of Justice (ojp.gov).

candidate's A-File information, reviews the candidate's criminal history—including any issued charging document(s) and any release paperwork—for accuracy and completed service, and updates the candidate's case file in ICE's Enforce Alien Removal Module.[16] Enforcement and Removal Operations constantly works to improve accuracy in the Enforcement Alien Removal Module to minimize the risk of releasing an ineligible candidate based on erroneous information.

During an initial check-in, as well as during any subsequent meetings with the participant, ICE ATD Case Managers explain the ICE ATD program to the participant, including their opt-out options and reporting requirements. The ICE ATD Case Manager completes the Form 71-015A, *ICE ATD Participant Enrollment Form*, with information maintained in ICE's Enforce Alien Removal Module and verifies the information with the ICE ATD participant. The ICE ATD Case Manager also selects and informs the participant of the frequency and type of visits (i.e., home or office visits) and the type of technology assigned (e.g., global positioning system ankle monitor, mobile device application or telephonic reporting).

To participate in the ICE ATD program, a participant must agree to and sign the *ICE ATD Enrollment From; Notice to Alien* ("ICE ATD Acknowledgement"), acknowledging their participation in the ICE ATD program; and the Intensive Supervision Appearance Program's *Program Rules Agreement* ("Program Participation Agreement"), which establishes the program rules and participant rights. The ICE ATD Program Participation Agreement also specifies that the ICE ATD participant agrees to the conditions of enrollment and participation in the ICE ATD program as well as the conditions of release (e.g., electronic monitoring).

These documents are explained to the ICE ATD participant in detail, and if necessary, through an interpreter in the participant's preferred language. The ICE ATD participant's Case Manager provides the participant with both the Acknowledgement and Program Participant Agreement to read, acknowledge, and sign. The ICE ATD Case Manager retains the original signed Acknowledgement and Program Participation Agreement in the ICE ATD participant's immigration case file and provides the ICE ATD participant with a signed copy.

Information Collection for Enrollment

The ICE ATD Case Manager collects information about the participant using standard ICE forms for non-detained noncitizens and maintains the information in ICE's Enforce Alien Removal Module and/or the ISAP case management system. The ICE ATD Case Manager completes Form 71-015A. The information is needed to monitor and supervise the participant in the ICE ATD program (discussed above). The following information maintained on Form 71-015A is verified

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), RISK ASSESSMENT CLASSIFICATION ASSESSMENT (RCA 1.0), ENFORCE ALIEN REMOVAL MODULE (EARM 5.0), AND CRIME ENTRY SCREEN (CES 2.0), DHS/ICE/PIA-015(d) (April 6, 2012), *available at* https://www.dhs.gov/privacy-documents-ice.

with the ICE ATD participant, and a copy is provided to the ICE ATD Servicer:

- Participant's biographical information, including name, A-Number, date of birth, country of citizenship, gender, street address, phone number;
- Referral source, including Criminal Apprehension Program, National Fugitive Operations Program, detained docket, non-detained docket, ICE Homeland Security Investigations, CBP, and USCIS;
- Whether the participant is part of a family unit, also residing within the United States; and
- Stage of removal proceedings (pre-decision/post-decision/order of removal/appeal).

Form 71-015A also requires the ICE ATD Case Manager to identify the technology option utilized (if applicable) and type of required check-in, as well as other ICE ATD service options (discussed in further detail below) that are assigned to the participant.

Other data elements may be captured in the participant's case in the Enforce Alien Removal Module and may be accessed at any time by the ICE ATD Case Manager. Other data elements may include:

- Government identification numbers, including passport number, state identification/driver license number, A-Number, vehicle registration, license plate number, Enforce Alien Removal Module case number;
- Email address;
- Descriptive data, such as race, height, and weight;
- Employment information;
- Education information;
- Relatives' or other point of contacts' name and phone number;[17] and
- Biometrics captured by the ICE ATD Case Managers used only for subsequent facial or voice verification required for monitoring and supervision-related check-in events (discussed below).[18]

Extended Case Management Service and Wraparound Stabilization Services

Extended Case Management Service (ECMS) is a component of ICE ATD programs that uses enhanced case management services to assist in stabilizing participants, including vulnerable populations such as family units, to help participants comply with their release conditions and

[17] Points of contact are established both as emergency contacts and contacts to locate a participant who is suspected of absconding from the program.
[18] The captured biometrics are not retained or used by DHS/ICE for any other purpose.

Executive Office for Immigration Review orders.[19] Extended Case Management Service participants may include victims of domestic violence or sexual abuse, families with physical and/or mental illness, and/or adults who could benefit from receiving additional referral services or assistance (e.g., food, housing, healthcare) and may need special assistance during immigration proceedings. The case management aspect of Extended Case Management Service continues to be managed by the assigned ICE ATD Servicer and Enforcement and Removal Operations oversight staff.

Part of the Extended Case Management Service's case review includes referring all new participants enrolled into ICE ATD for a supplemental services evaluation. If a participant qualifies, ICE ATD Case Managers may offer targeted and specific Wraparound Stabilization Services for behavioral and psychological assistance provided by non-profit organizations. These non-profit organizations are sub-contracted by the ICE ATD Servicer. Wraparound Stabilization Services are an additional enhancement to the appropriate ICE ATD program that provide further targeted behavioral and psychological services not offered by Extended Case Management Service. Like Extended Case Management Service, Wraparound Stabilization Services are provided by non-profit organizations while the case management aspect continues to be managed by the assigned ICE ATD Servicer and Enforcement and Removal Operations oversight staff.

Family units are enrolled into Extended Case Management Service and Wraparound Stabilization Services under a head of household. The head of household provides family member information (e.g., names, dates of birth, relation, gender, A-Numbers), other biographical information, and criminal information to Extended Case Management Service and/or Wraparound Stabilization Services program staff. Once this information is collected, it is entered into the respective ICE ATD case management system and case management and program staff review cases for vulnerabilities, update or modify information based on face-to-face visits, and monitor technology and participant activities throughout the lifecycle of a participant's immigration case.

ISAP ATD Case Management System

The ISAP ATD program uses the ISAP ATD case management system, a cloud-based information technology platform designed to facilitate the seamless entry, modification, and querying of data for ICE ATD case management. The platform's capabilities include the tracking and monitoring of case management services, electronic monitoring functions, such as proprietary global positioning system cellular technology, and voice verification biometric products used for telephonic check-ins. In addition, the platform provides ICE ATD Case Managers with access to vendor-operated open-source (e.g., commercial) data aggregator services. Such services include, for example, a nationwide database, assembled by direct connections to 2,800 U.S. incarceration

[19] ICE defines a "family unit" as an adult noncitizen parent or legal guardian accompanied by their own juvenile noncitizen child(ren).

facilities, that provides information on whether ICE ATD participants are incarcerated or have prior incarcerations. The aggregator services support ICE ATD Case Managers' efforts to monitor the participants' compliance with requirements concerning their immigration-related schedule (e.g., court hearings, home, or office visit, and/or check-in with ICE ATD Case Manager/ICE ATD field office) and other release conditions. While the ICE ATD Servicer is the data custodian, ICE is the owner of all data generated and maintained in the ISAP ATD case management system.

ISAP - ICE ATD Electronic Monitoring

The ICE ATD program uses data aggregator services, global positioning system cellular technology, or biometric verification technology (i.e., voice and facial verification) products to support its monitoring and supervision efforts. ICE ATD Case Managers use these technologies to verify the status, location, and identity of the participants during check-in, as described below.

Data Aggregator Service – ICE ATD's use of Commercial and Open-Source Data

The ICE ATD Servicer utilizes a third-party data aggregator service maintained within the ISAP ATD case management technology platform, which allows the ICE ATD Servicer to query a searchable commercial database for nationwide criminal booking information, to monitor if participants have been arrested. The ICE ATD Servicer inputs basic biographic information into the data aggregator service (e.g., name, date of birth), and the data aggregator service searches for any matches within the commercial database. If the biographic details of a criminal arrest or criminal booking event in the commercial database match biographic information for an ICE ATD participant, the data aggregator service securely transfers, in real time, all available details of the event to the ICE ATD Servicer. Such details may include biographic information, the booking facility information, and the alleged crime associated with the booking.

The data aggregator service's query returns will specify which data elements were matched and the system's confidence score as to the reliability of the match. Logged matches and the associated confidence score are recorded as an event in the ICE ATD Servicer's platform. The ICE ATD Servicer is required to verify a match provided by a data aggregator service by conducting independent verification, including through open sources if necessary, and documenting the other verification information upon which the ICE ATD Servicer relied. Once confirmed, the ICE ATD Servicer creates a report for an Enforcement and Removal Operations ICE ATD field office review. This report will include the data aggregator service's query returns and the ICE ATD Servicer's analysis confirming whether the return matched the identified participant.

The ICE ATD field office may not rely solely on information provided by the ATD Servicer and must conduct its own criminal history checks prior to taking an enforcement action. Enforcement and Removal Operations ICE ATD field offices may enter the ICE ATD Servicer's report into the Enforce Alien Removal Module if the results are relevant to an Enforcement and Removal Operations enforcement activity. In that event, the report is treated as an investigative

lead if Enforcement and Removal Operations takes enforcement action (e.g., arrest, termination of participant from ICE ATD).

Global Positioning System Cellular Ankle Monitor Units

A global positioning system unit may be assigned to an ICE ATD participant to ensure compliance with terms of the participant's release. Participants are given notice that tampering with or damaging the unit may result in arrest, detention, and prosecution. The global positioning system unit is secured to the participant's ankle and has a unique serial number associated only with the assigned participant in the ISAP ATD case management system. The ankle monitor continuously tracks and logs in the ISAP ATD case management system GPS points. ICE ATD Case Managers may track, in real time, the location of the participant by querying a global positioning system unit's unique serial number in the ISAP ATD case management system. Each query of the participant's location by a case manager is recorded in the system as an event and subject to auditing.[20] The ICE ATD participant's location is tracked by—latitude and longitude coordinates—provided through global positioning triangulation via satellites, cell tower triangulation via cell towers, and Wi-Fi positioning technologies.

In addition, ICE ATD Case Managers can view, search, and review the participants' historical ICE ATD location data via the ISAP ATD case management system by retrieving the participants' record at any time by querying a name, date of birth, A-Number, or Enforce Alien Removal Module case number. The ICE ATD Case Manager can program a global positioning system unit to monitor a participant's whereabouts according to a specified "inclusion" or "exclusion" zone set in the participant's case.[21] An inclusion zone alert notifies the ICE ATD Case Manager that a participant has left an assigned zone. An exclusion zone alert notifies the ICE ATD Case Manager that a participant has entered a specified, unauthorized area. Finally, ICE ATD Case Managers can send pre-programmed recorded messages (e.g., "contact ICE ATD immediately") to the participants via the global positioning system unit, which beeps at regular intervals until the participant acknowledges delivery.

Telephonic Reporting – Voice Biometric Product

ICE ATD Case Managers may decide a participant need only be monitored by regular telephone check-in. For this type of monitoring, the ISAP ATD case management system sends an

[20] ATD Case Managers may only query an ATD participant's current and historical global positioning system unit in accordance with ICE policy, such as if the ATD participant cannot be located or failed to appear at a court hearing. ATD policy requirements and restrictions will be included in the forthcoming ICE Non-detained/ATD standards.
[21] Inclusion/exclusion zones are established by the Enforcement and Removal Operations and conveyed to the case manager. The goal of an inclusion zone it to notify the case manager or the ATD officer that a participant has left a specified zone, and the exclusion zone setting accomplishes the opposite goal. The exclusion zone is primarily used for participants leaving the SWB, and once the participant arrives at their intended destination city the ATD officer is notified. The inclusion zone establishes a boundary, which is generally the state in which the participant resides. The participant must request approval prior to leaving the boundary or an alert is generated.

automated call to the participant's listed phone number at a pre-determined monthly check-in time. When the participant answers, the system matches the responding individual's voice against the pre-recorded voice print that the ICE ATD Case Manager collected during intake and enrollment. The pre-recorded voice print is the only voice print recorded and securely stored in the ISAP ATD case management system.[22] The stored, pre-recorded voice print is not used for any purpose other than to verify the identity of the individual answering the check-in call. The ICE ATD Case Manager will receive an alert via the ISAP ATD case management system notifying them whether the voice verification was successful or unsuccessful. If the voice verification is unsuccessful, or there is a technical issue, the ICE ATD Case Manager will reach out to the participant to attempt resolution.

Monitoring Mobile Application

The ICE ATD program may use a mobile application (referred to in this document as "Monitoring App")[23] to monitor participants using voice or facial verification functions at the time of check-in. Participants either receive an issued ICE ATD Servicer device (i.e., phone with the Monitoring App pre-installed) or install the app on their own device. Participants using the ICE ATD-issued devices can only use the Monitoring App to communicate with the ICE ATD Case Managers, and to make 911 emergency calls.

If participants agree, the ICE ATD Case Manager may instead install the Monitoring App on the participant's personal phone. The Monitoring App can be downloaded from the Apple and Android Play stores. However, the Monitoring App can only be accessed and used by ATD participants who are registered in the ISAP ATD case management system. If a non-registered individual downloads the Monitoring App, they will not be able to use the application. Following download, the ATD participant will receive login credentials after the ATD participant is authenticated by the ISAP ATD case management system. The ATD participant's personal phone must also meet the minimum technical specifications required by the Monitoring App. Finally, the Monitoring App is specifically designed to prohibit access to other aspects of a participant's personal mobile device, such as contacts, photographs, and messaging apps.[24]

Use of the Monitoring App, whether through an ATD-issued device or the participant's personal device includes a requirement that the phone's location services function be enabled. The

[22] The captured voiceprint is not retained or used by DHS/ICE for any other purpose.
[23] The ICE ATD monitoring mobile application is proprietary technology also known as BI's SmartLink, which was developed as an extension to the ICE ATD case management system. This Privacy Impact Assessment will continue to refer to the application as "Monitoring App" for the duration of the document to account for the fact that in the future the application may be renamed or replaced.
[24] As noted previously, ICE ATD policy requirements and restrictions will be included in the forthcoming ICE Non-detained/ATD standards. In the meantime, as discussed below, the mobile app includes security features that prohibit access to information on the participant's mobile device, with the exception of location data points when the app is open.

ATD Case Manager does not receive constant location data from the ATDs participant's device. The ATD participant's location data—longitude and latitude coordinates—are only sent to the ATD Case Manager when the ATD participant signs into the Monitoring App and completes a check-in. Additionally, the ATD Case Manager can send a prompt to the ATD participant to request a check-in (e.g., if participant missed a hearing or ATD Case Manager reasonably believes the participant may have absconded). Once the ATD participant signs into the Monitoring App and complete the check-in, the Monitoring App sends the phone's location data via satellite technology to the ICE ATD Case Manager to verify that the participant's location is not outside the "inclusion zone" or geographic radius established and identified during enrollment.

Facial Verification Feature

The Monitoring App also includes unique facial verification technology that allows participants to capture their photo during ICE ATD enrollment for future verification purposes (e.g., during check-in). Unlike facial identification—also known as facial recognition—the facial verification function within the Monitoring App is not used to confirm the individual's identity using facial recognition. Rather the Monitoring App uses a one-to-one matching approach of the individual presenting to the Monitoring App during their check-in by comparing it against the ATD participant's photograph captured upon enrollment to determine whether the person is who they declare themselves to be. the. The Monitoring App—whether it is launched from an ICE ATD-issued mobile device or from the participant's personal mobile device—takes a series of photos of the participant during enrollment. The photos are also stored in the ISAP ATD case management system. When the participant subsequently checks in, an automatic 1:1 verification image of the individual in front of the phone's camera is matched against the stored profile images to enable the ICE ATD Case Manager to verify the participant's identity, using a proprietary algorithm. The technology also recognizes if a "live" person is in front of the camera, as opposed to a representation or image of a person. There is only a visual ICE ATD Case Manager review if there is no match or if the matching attempt generates an error alert. The photos are only used for the described verification purpose and are not shared for any other purpose or with any other entity or database. Any pictures taken during the facial template capture are immediately deleted from the device and only the facial measurements are captured.

Messaging and Video Conferencing Functions

The Monitoring App allows the ICE ATD Case Managers to communicate using the two-way messaging and video conferencing functions within the App, such as sending and receiving check-in alerts, and scheduling reminders. If the ICE ATD participant chooses to install the Monitoring App on their personal cell phone, the ICE ATD Case Managers are prohibited from accessing any other data stored in, or generated by, the participant's personal mobile device (e.g., personal emails, text messages, phone conversations, phone numbers called or received, pictures sent or received) and the Monitoring App has security safeguards in place to prevent such access.

In addition, the video conferencing feature allows the ICE ATD Servicer to conduct case management video conferences with the participant as necessary. The video conferencing feature does not include the ability to record and store meetings. This feature is only used as a way to communicate with the ICE ATD participant, such as during a USCIS credible fear determination as discussed below.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[25] 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. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is managed in full compliance with the fair information practices as set out in the Privacy Act of 1974.[26]

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.[27] 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 Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[28] and the Homeland Security Act of 2002, Section 222.[29] Because YACMP and ISAP are ICE ATD programs, rather than a particular information technology system, this Privacy Impact Assessment examines privacy risks associated with the programs and related mitigation measures pursuant to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information. Technologies or systems using personally identifiable information must be described in a System of Records Notice (SORN) and PIA, as appropriate.

---

[25] 5 U.S.C. § 552a.
[26] 6 U.S.C. § 142(a)(2).
[27] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFOMRATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DPEARTMENT OF HOMELNAD SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[28] 44 U.S.C. § 3501 note.
[29] 6 U.S.C. § 142.

Under YACMP, ATD participants proceed through an orientation process and the information about the individual provided by the referring entity is confirmed with the ATD participant in an in-person enrollment meeting with an ICE ATD Case Manager. During the enrollment meeting, additional information (identified above) about the ATD participant is collected and used to complete the YACMP-related forms. Under ISAP, the ICE ATD Case Manager completes Form 71-015A with information about the participant maintained in ICE's Enforce Alien Removal Module and confirms the accuracy of that information with the ICE ATD participant. For both the YACMP and ISAP programs, the ICE ATD Case Manager explains the program and outlines the conditions of the participant's ongoing enrollment in ICE ATD (e.g., type of monitoring, frequency of check-ins, important dates). If the ATD participant is enrolled in ISAP, the ICE ATD Case Manager also describes the technology to be assigned to the participant, and instructs the participant on how to use the technology.

All ATD meetings are conducted in the participant's preferred language, using interpreters, if necessary. Participants are then given the ICE ISAP ATD Program Participant Agreement or YACMP Program Orientation Attestation Form to read and sign. The agreements notify participants that the consequences of failure to comply with the requirements of the ICE ATD program may result in a re-determination of their release conditions, arrest, and detention.

Under ISAP, ICE ATD participants who are fitted with a global positioning system ankle tracking device are instructed that their location always will be monitored, and that ICE ATD Case Managers may be able to search the history of the participant's device for the length of their enrollment in the ICE ATD program. Participants who are monitored by an electronic Monitoring App are advised to respond promptly to check-ins at the pre-determined monthly check-in time using the facial or telephonic verification functions or face the consequence of arrest, detention, and prosecution. Additionally, the ISAP ATD participant is informed that the Monitoring App sends an alert to the ISAP ATD case management system if the participant travels outside of the assigned geographic area and into an exclusion zone location. ISAP and YACMP participants are notified that ICE ATD Case Managers have their contact and location information so that the Case Manager can follow up if the participant misses a call-in.[30]

ICE also provides general notice of the ICE ATD programs by the publication of this Privacy Impact Assessment. In addition, the information collected and used by each ICE ATD program and maintained in YACMP and ISAP ATD case management systems and ICE systems is covered by the following Privacy Impact Assessment and Systems of Records Notice related to their respective IT systems.

[30] YACMP does not use the ISAP Monitoring App or other forms of electronic monitoring technology. As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements set forth under the non-detained docket management process.

- DHS/ICE/PIA-015 Enforcement Integrated Database (January 14, 2010), and subsequent updates;[31] and
- Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records Notice, which covers the identification, arrest, charging, detention, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive noncitizens and undocumented re-entrants.[32]

Privacy Risk: There is a risk that participants may not know, or understand, the terms and conditions of participation in an ICE ATD program, or what data ICE is collecting through its monitoring services.

Mitigation: This risk is partially mitigated. ICE ATD Case Managers collect information directly from the ICE ATD participant during an in-person enrollment meeting. During this in-person meeting, the ICE ATD Case Manager explains the rules of the ICE ATD program, such as the reporting and check-in requirements and/or assigned technology and the frequency of the home or office visits; the information that is being collected and the purpose for collection; and the consequences of failure to abide by the terms of the ICE ATD program requirements and conditions of release. If necessary, this meeting is conducted in the participant's preferred language, using an interpreter.

In addition, the ICE ATD participant is given a copy of all enrollment-related documents, and the participant signs and acknowledges receipt and understanding of the ICE ATD program agreement and attestation forms. These documents identify the types of information collected and the purpose for the collection. If an interpreter is required, one is provided to assist with review and understanding of the documents. Finally, the risk is further mitigated through regular home or office visits with the ICE ATD Case Manager as part of the monitoring and supervision process, during which the Case Manager can assess the participant's understanding of and answer any questions the participant may have about the ICE ATD program.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using personally identifiable information. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of personally identifiable information and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of

[31] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015 (January 14, 2010, and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[32] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

personally identifiable information.

As noted above, prior to and during the ICE ATD enrollment process, the participants' referral source (e.g., a DHS Component) and the ICE ATD Case Manager meet with the participant and explain the ICE ATD program in detail. ICE ATD Case Managers review the goal of the program, which is to assist the participant in complying with release conditions. For ISAP participants, Case Managers also review the use of technology to monitor/supervise the participant to help achieve the compliance goal. The ICE ATD Case Manager also explains to the participant the consequences of not abiding by the terms of the program. At this point, the individual can choose to opt out of the ICE ATD program. A decision to opt out results in the usual non-detained docket requirements, including annual check-in requirements or depending on the circumstances, the individual may be detained for the duration of their immigration case.

If the individual elects to enroll in an ICE ATD program, the ICE ATD Case Manager will complete Form 71-015A or YACMP-related forms mentioned above. The ICE ATD Case Manager explains to the ATD participant, the reporting requirements, as well as the frequency and type of required in-person check-in (home or office visits), and/or the assigned technology (global positioning system, electronic monitoring through the mobile app, and/or biometric voice check-in). The ICE ATD Case Manager will explain the contents of the ICE ATD Program Participation Agreement or YACMP orientation and other YACMP-related documents and forms in the participant's preferred language through a language or sign language interpreter, if necessary, and obtain the participants signature, acknowledging receipt and understanding of the ICE ATD program. After enrollment, the ICE ATD Case Manager has regular contact with the participant, and the ATD participant can clarify any issue, including questions about the assigned technology.

Under ISAP, the ICE ATD participant, at the time of enrollment into the ICE ATD program, signs Form I-220A, *Order of Release on Recognizance*; Form I-220B, *Order of Supervision*;[33] and the ICE ATD Program Participant Agreement, which specifies conditions of enrollment and participation and the conditions for release. These documents acknowledge the participant's understanding of the conditions of the ICE ATD program. An ICE ATD participant is notified of their right to object to any new conditions of release imposed upon them during their enrollment in the program, or object to termination from the ICE ATD program in which they are enrolled. In these situations, an ICE ATD participant may:

- File an application to improve their terms of release with the Executive Office of Immigration Review;

[33] Form I-220A, *Order of Release on Recognizance*; Form I-220B, *Order of Supervision*; Form I-830-e, *Notice to EOIR, Alien Address*.

- Submit a written request for reconsideration of the new reporting or monitoring requirements to the ICE ATD Case Manager; or
- Submit a written request for reconsideration to the ICE ATD supervisor.

Individuals seeking notification about and access to the records covered by this Privacy Impact Assessment may submit a request in writing to the ICE Freedom of Information Act (FOIA) Officer by mail or facsimile to:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
Fax: (202) 732-0660
http://www.ice.gov/foia/

Individuals seeking to correct or contest the records contained in a system of records may submit a Privacy Act request in writing to the ICE Office of Information Governance and Privacy by mail to:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy Attn: Privacy Unit
500 Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

All or some of the requested information may be exempt from correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests.

If individuals believe more than one DHS component maintains Privacy Act records concerning them, they may submit the request electronically to the DHS Chief Privacy Officer, at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form or mail a request to:

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Privacy Risk: There is a risk that ISAP ATD participants' associates or family members will not have the opportunity to consent to ICE ATD program collection of their personal information.

Mitigation: This risk is partially mitigated. Noncitizens are provided the option to participate in an ICE ATD program. ATD participation includes providing contact information for family members to be used only in the event the ATD participant cannot be located (e.g., failed to attend a court hearing, device malfunction). If a participant does not consent to the collection of

their information and emergency contact list information, they are not permitted to participate in the program. Although the ATD participant's associates and family members cannot directly consent to collection of their information, emergency contact information is coordinated and obtained with the participant's consent with the understanding that these individuals may be contacted and the contact information is only used in cases when the participant is out of communication with the ICE ATD program (e.g., failed to attend a scheduled court hearing). This Privacy Impact Assessment provides notice to potential contacts of participants that their information could be collected by the ICE ATD program.

Privacy Risk: There is a risk that the ICE ATD participants may not understand the ICE ATD program and the consequences of their violation of its terms.

Mitigation: This risk is partially mitigated. Noncitizens are provided with an interpreter if needed, and all ICE ATD Case Managers are trained to carefully explain the terms of ICE ATD programs. All participants opt into the ICE ATD program during enrollment, and only do so after it is clear to the ICE ATD Case Manager that the noncitizen understands the ICE ATD program terms and conditions of release. Further, the ICE ATD Case Manager has regular contact with the participants and can verify and further clarify participants' understanding of the ICE ATD program as needed. The ICE ATD Case Manager will also observe whether the participants understand the requirements of the program and provide additional clarification during check-ins. Finally, the ICE ATD participant is provided a copy of the ICE ATD Program Participant Agreement or YACMP Program Orientation Attestation Form after signing.

Privacy Risk: There is a risk that ICE ATD participants may not be able to access or amend their ICE record(s). If ICE records are inaccurate, this could lead to issues such as misidentification or an inability for a participant to fulfil their responsibilities under the program.

Mitigation: This risk is partially mitigated. For information collected and maintained under the ICE ATD program, individuals can submit requests to ICE to access, correct, or contest their records. Under DHS policy, ICE treats all records about noncitizens as if they were covered under the Privacy Act, regardless of immigration status. Accordingly, all individuals have the option of correcting inaccurate information in their ICE records, unless these records are exempt under the corresponding System of Records Notice (e.g., law enforcement investigations). ICE will also consider requests to correct an individual's record in the Enforce Alien Removal Module or ICE ATD case management system, if the individual provides ICE with information establishing the inaccuracy of ICE's records.

3. Principle of Purpose Specification

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

DHS is authorized to collect information for the ICE ATD program under 5 U.S.C. § 301; 8 U.S.C. § 1103; 8 U.S.C. § 1360(b); 8 U.S.C. §§ 1365a and 1365b; 19 U.S.C. § 1; and 19 U.S.C. §§ 1509 and 1589a. Additional authority is provided in 6 U.S.C. § 202; 8 U.S.C. §§ 1158, 1201, 1379, and 1732; and 19 U.S.C. §§ 2071, 1581-1583, and 1461; and the Immigration Reform and Immigrant Responsibility Act of 1996.

Privacy Risk: There is a risk that information collected from participants in the ICE ATD program and through monitoring or tracking activities will be collected and used in a manner inconsistent with the purposes for which its collection and use is authorized. This includes risks that information may be misused for unauthorized persistent monitoring.

Mitigation: This risk is partially mitigated through training, access control, and management oversight to ensure that ICE personnel use data only for purposes that are consistent with ICE's authority to collect and use the information.

Training

ICE, by policy, requires all ICE personnel (federal contractors and employees) to complete DHS Annual Information Assurance Awareness Training and DHS Privacy Training, which stress the importance of appropriate and authorized use of personal data in government information systems. ICE has ensured, via contract, that personnel employed by the ICE ATD Servicer handling personal information are required to and in fact complete the training as well.

Access Control

ICE ATD user access roles are in place to mitigate the risk of unauthorized individuals gaining access to ICE ATD case managements systems. Role-based access is granted to authorized personnel with a need to know and is constrained to their specific user roles and responsibilities. Information collected is only shared with the ICE ATD Case Managers that have a need-to-know to enable them to perform their duties under the ICE ATD program.

Management Oversight

Enforcement and Removal Operations officers assigned to an ICE ATD program ensures the training of all personnel and are instructed to collect and use information only to the extent required to enroll the participants in an ICE ATD program and to monitor and supervise them while they are in the program. The ICE ATD Servicer is also required by their contract with ICE to only use the information to the extent necessary to fulfill their contractual duties.

Technology Restrictions

YACMP does not use the ISAP Monitoring App or other forms of electronic monitoring technology. As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements

set forth under the non-detained docket management process. As part of the non-detained docket management process, ICE will conduct criminal background checks to ensure YACMP participants have not allegedly violated any criminal laws while participating in the ICE ATD program.

Under ISAP, persistent monitoring is necessary for ICE ATD participants using a global positioning system device. As noted above, participants using this technology are notified during enrollment, and in subsequent meeting check-ins, that there will be persistent monitoring. For ICE ATD participants that are issued an ICE ATD device with the pre-installed Monitoring App, the Monitoring App only provides their location data point via satellite technology when the applicant is either logging into the Monitoring App from their personal mobile device and/or at the time the ATD participant completes the biometric check-in, to determine whether the participant is within the pre-approved geographic area established during enrollment. Regardless of whether the ICE ATD participant is assigned an ICE ATD device or agrees to install the Monitoring App on their personal cell phone device, the ICE ATD Case Manager is prohibited from receiving geolocation data other than the longitude and latitude coordinates of the ATD participant. Further, geolocation data is only transmitted to the ATD Case Manager when the participant logs into the Monitoring App and/or when a biometric check-in is completed. This is the case regardless of whether the ATD participant leaves the Monitoring App running in the background. In addition, the Monitoring App will send an alert to the ATD Case Manager via the appropriate ICE ATD case management system notifying them that the ICE ATD participant is outside the approved geographic area only at the time of check-in. In other words, the Monitoring App is not continuously monitoring the participant's location. Finally, the Monitoring App is specifically designed to prohibit access to other data on a participant's personal mobile device.

Privacy Risk: There is a risk that information collected by ICE ATD programs will be stored in other ICE and DHS databases and used for other DHS mission purposes.

Mitigation: This risk is partially mitigated. In accordance with the One DHS Memo,[34] in order to promote a united, Department-wide information sharing environment, it is critical that each DHS component gives the highest priority to sharing of potential terrorism, homeland security, law enforcement, and related information with other DHS components. DHS personnel must have timely access to all relevant information for which they have a need-to-know to successfully perform their duties. Therefore, absent any legal prohibitions, and in accordance with laws, regulations, policies and ICE and Department System of Records Notices, information is shared within DHS only for authorized purposes and in a manner that safeguards and protects the information.

[34] One DHS Memo, "DHS Policy for Internal Information Sharing and Exchange," Feb. 7, 2007.

4. Principle of Data Minimization

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

The ICE ATD programs only collect the participants' personally identifiable information that is relevant and necessary to their monitoring and supervision while enrolled in an ICE ATD program. The information collected is used to track the ICE ATD participant's compliance with requirements for being present or appearing at certain locations (e.g., home, ICE ATD office, court hearing) and/or checking in with ICE ATD Case Managers. The collected information also allows ICE ATD to track any extended case management and/or wraparound stabilization service options provided to the participant. While the biographical information of the type listed in Form 71-015 or YACMP-related forms is collected from all enrollees, any additional information collected from an ICE ATD participant is only collected depending on the type of case management or monitoring they are assigned.

For telephonic reporting, ISAP ATD participants provide a voice print at the time of enrollment to allow the voice of the individual calling in for telephonic reporting to be matched against the voice print provided during enrollment. For global positioning system ankle monitor tracking, the device tracks whether the ISAP ATD participant is traveling within the geographic area assigned during enrollment and notifies the ICE ATD Case Manager if the participant entered or left pre-determined zones. For those ISAP ATD participants assigned the Monitoring App, the app on the participants' personal mobile device will collect location information and notify the ICE ATD Case Manager at the time of check-in whether the participant is checking in from the location specified in the participant's release.

Upon enrollment, the Monitoring App also uses the device's camera to capture the participant's facial measurements (a template) from a series of photographs. This facial biometric is used to verify the participant's identity for ISAP ATD program check-in purposes only. Any pictures taken during the facial template capture are immediately deleted from the device and only the facial measurements are captured. The measurements are stored within the app and used to compare subsequent check-in photographs to validate a facial template match for facial verification purposes. The Monitoring App uses facial verification to determine the live individual is in front of the device at the time of check-in, not simply a photo or print of the individual.

Until the YACMP ATD case management system can be linked with ICE's Enforce Alien Removal Module, ICE ATD program records contained in the YACMP ATD case management system will be retained permanently. ICE ATD program records contained in the ISAP ATD case

management systems or maintained in paper-based files are destroyed (e.g., removed from the system or shredded) seven years after the cutoff date, which is the date on which the participant is terminated from the ICE ATD program. This includes information collected within ISAP's Monitoring App, which is transmitted to the ISAP ATD case management system. With an ICE Records Officer approval, Enforcement and Removal Operations completes a form instructing the ICE ATD Servicer to terminate a participant from an ICE ATD program. The ICE ATD Servicer documents Enforcement and Removal Operations' termination instruction, which triggers an alert (a hard date locked into the ICE ATD Servicer's system) informing the ICE ATD Servicer to destroy the records seven years after the termination date. The alert prompts the ICE ATD Servicer to run analytics to identify these records for destruction.

The ISAP ATD program records are an extension of the ICE Enforcement and Removal Operations Enforce Alien Removal Module system and maintained in ICE's Enforcement Integrated Database. All records maintained under ICE ATD programs, which are in ICE systems, fall under the Enforcement Integrated Database retention schedule. The records retention schedule is DAA-0567-2018-0001-0001 Participant Tracking Records, and DAA-0567-2018-0001-0002 Incident/Violation Reports, which requires records to be destroyed 75 years from the date of entry.[35] The records listed above with a seven-year cutoff are manually destroyed after the retention period is complete. Records in Enforcement and Removal Operations' Enforcement Integrated Database/Enforce Alien Removal Module are automatically purged from the system according to their retention schedules.

Privacy Risk: There is a risk that ICE ATD programs will over-collect information from the participants (i.e., collect more information than is needed for the purposes of the ICE ATD program).

Mitigation: This risk is mitigated. ICE ATD programs collect only the information and data necessary to ensure successful enrollment in and participant compliance with an ICE ATD programs' requirements, including reporting check-in requirements and other conditions of release. The ICE ATD Case Managers' use of Form 71-015 and YACMP-related forms has proven effective in collecting only the type of information that allows the ICE ATD Case Managers to monitor and supervise the ATD participants in their respective ICE ATD programs. Additional data is only collected from a participant to the extent it is required for the type of case management or monitoring to which they are assigned.

YACMP does not use the ISAP Monitoring App or other forms of electronic monitoring technology. As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements

[35] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2018-0001_sf115.pdf.

set forth under the non-detained docket management process.

Finally, the ISAP technology such as the Monitoring App and global positioning system tracking are limited through both technical and policy restrictions to collect only what is needed for the ICE ATD program to function effectively. ATD Case Managers can track, in real time, the location of the participant by querying a global positioning system unit's unique serial number in the ICE ATD case management system.[36] ATD Case Managers may query an ATD participant's global positioning system unit in accordance with ICE policy, such as if the ATD participant cannot be located or failed to appear at a court hearing. The ATD Case Managers are not permitted to use the Monitoring App to continually track the ATD participant's location. The Monitoring App is contractor-owned, proprietary technology and its functionality is customized for ICE's use to meet the ICE ATD program requirements. The Monitoring App's technology is designed to only send the ATD participant's location data point—longitude and latitude coordinates—at the time the individual logs into the application and at the time of check-in. Therefore, these security features prevent the ATD Case Manager from obtaining the ATD participant's location data at any time other than when required under the program.

Privacy Risk: There is a risk that under ISAP, ICE ATD Case Managers will collect information from an individual's personal mobile device, including collecting images and/or audio of non-participants during check-ins using the Monitoring app and/or telephonic check-in.

Mitigation: This risk is mitigated. As noted above, for ICE ATD participants who agree to install the Monitoring App on their personal cell phone device, the ICE ATD Case Manager does not receive constant location data from the Monitoring App. Rather, the ICE ATD Case Manager may send a prompt to the ATD participant to request a check-in (e.g., if a participant missed a hearing or the case manager reasonably believes the participant may have absconded). Once the ATD participant signs into the Monitoring App and completes the check-in, the ICE ATD Servicer we will receive location coordinates back and map them for the ICE ATD Case Manager to confirm the individual is within the assigned geographic area at the time of check-in. In addition, the Monitoring App is specifically designed to prohibit access to other aspects of a participant's personal mobile device, this includes access to their contacts, photos, texts, and other information maintained on the ICE ATD participant's personal cell phone device.

For participants using the Monitoring App for facial verification check-ins, the camera is only active when the application is open (the application times out after 30 minutes). The Monitoring App does not have the capability to access the camera outside of the ICE ATD application's use of the application, and images captured at the time of check-in are only used to compare against facial measurements created from photographs taken during enrollment. These

[36] ATD policy requirements and restrictions will be included in the forthcoming ICE Non-detained/ATD standards.

photograph - both taken at the time of enrollment and for check-in purposes - are not recorded or maintained in the Monitoring App, though the biometric print/face measurement is.

Participants using the telephonic check-in voice verification provide voice-print samples upon enrollment. While the enrollment voice prints are recorded and maintained, the voice prints provided during the check-in process are not recorded or retained. As discussed above, if the voice print used during check-in fails the voice biometric verification process, an alert is sent to the ICE ATD Case Manager via the appropriate ICE ATD case management system notifying the ICE ATD Case Manager of an unsuccessful check-in.

Privacy Risk: There is a risk that ICE retains information for longer than is required for the purposes for which the information was collected.

Mitigation: This risk is partially mitigated. As noted above, the ICE ATD program records are an extension of ICE's Enforce Alien Removal Module and fall under the Enforcement Integrated Database retention schedule. ICE's Enforcement Integrated Database alerts users to destroy the records 75 years from date of entry. Upon system user notification, the records are manually deleted from the system. Records held in the ICE ATD Servicer's Case Management System are destroyed seven years after participant termination from the program.

Privacy Risk: There is the risk that the ICE ATD Servicer may retain records—either on its system or in hard copy—and would not properly dispose of the records when the retention period ends, despite the relevant provisions in the ICE ATD Servicer's contract with ICE.

Mitigation: This risk is partially mitigated. The ICE ATD Servicer has the contractual obligation to maintain and purge records as provided in the contract. Enforcement and Removal Operations' termination instruction (after ICE Records Officer authorization) triggers an alert to the ICE ATD Servicer destroy all records seven years after the termination date would, including any paper records the ICE ATD Servicer may have in its possession. The ICE ATD Servicer is required to submit a records disposition when the contract ends.

5. Principle of Use Limitation

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

The information collected is used to identify, monitor, supervise, and assist the participants in complying with the YACMP or ISAP ATD program's requirements and the conditions of the participant's release into the community pending resolution of their immigration case. The information can also be used to detain, apprehend, and remove the participants from the United States should they fail to comply with the terms of the YACMP or ISAP ATD programs or the

conditions of their release, or in the event a final order of removal is issued.

For ISAP ATD participants who have filed an application for asylum, USCIS, in partnership with ICE ATD Case Managers, uses the video conferencing feature in the electronic Monitoring App to enable USCIS to conduct credible fear interviews remotely, and in a non-detained setting. USCIS does not operate the Monitoring App. ICE ATD will operate the Monitoring App in the case of a video conference and invite USCIS to participate in the conference. USCIS only views the conference to ensure the ICE ATD participants are not being coached during the interview and enable USCIS to make a credible fear decision; USCIS does not collect personally identifiable information from this encounter.

Privacy Risk: There is a risk that the information the ICE ATD Case Managers collect from or about the participants could be used beyond an ICE ATD program's goals, including the improper use of the information obtained from the ATD participants, such as an ISAP participants' contact information on family and friends.

Mitigation: This risk is partially mitigated. The Monitoring App, which can be loaded onto the participant's personal mobile device for ICE ATD compliance, is specifically designed and purposely limited in its features and capabilities to collect only the information and data necessary to provide oversight and facilitate the participants' compliance with the ICE ATD program. The Monitoring App is designed and limited to the functions which increase the participants' rate of compliance with their release conditions by providing routine monitoring and supervision services, including reminders of court and check-in appointments, home visits, school obligations, and curfew rules, if applicable.

The ICE ATD participant also provides emergency contact information for individuals (family and friends) in the event the ICE ATD Case Manager cannot locate the participant. The ICE ATD Case Managers only contact individuals on the participants' contact list for the purpose of locating a participant whose whereabout is unknown. For example, before taking a law enforcement action, the ICE ATD Case Manager will contact these individuals if the participant misses court hearings or an ICE ATD check-in, or if the participant cannot be located after all other attempts at contact have been exhausted. This limitation is enforced through training, access control, and management oversight as described above.

Privacy Risk: In the case of the participants who elect to have the Monitoring App installed on their own personal mobile devices (rather than accept an ICE ATD-issued device which is pre-loaded with the Monitoring App), there is a risk that the Monitoring App on the participants' personal mobile device may allow the ICE ATD Case Manager access to other personal applications on the participant's phone, including access to the participants' private activities beyond their transaction with the ICE ATD Case Manager for ICE ATD business (e.g.,

the participants' private phone calls, phone numbers called or received, text messages sent or received, and pictures sent or received).

Mitigation: This risk is mitigated. The Monitoring App has been designed and developed to preclude access to any data on the participants' personal devices not related to ATD purposes discussed in this Privacy Impact Assessment. It is a compartmentalized application which cannot access any mobile device resources or stored personal data. As such, it is a self-contained application that exclusively utilizes resources contained within the Monitoring App. The Monitoring App, available in the Apple and Android Play stores, describes the application's limited access to location data and the participant's contact information.

Privacy Risk: There is a risk that information may be shared with external parties who do not have a need to know.

Mitigation: This risk is mitigated. ICE does not share any information collected under ICE ATD programs without the participant's consent, unless there is an applicable Privacy Act exception, such as a routine use listed in the relevant System of Records Notice, or as otherwise required by law and policy.

6. Principle of Data Quality and Integrity

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

The ICE ATD Case Managers collect biographical data directly from the ISAP and YACMP ATD participants during enrollment at the in-person intake meeting to manage and track the participants' compliance with release conditions. During ISAP ATD program enrollment, ICE ATD Case Managers collect biometric information in the form of facial metrics measurements and voice print for purposes of identity verification during subsequent check-in. They also search DHS/ICE systems (e.g., Enforce Alien Removal Module) to locate participant information that is already stored in the systems.

Privacy Risk: There is a risk that the technology assigned to ISAP participants, such as the global positioning system ankle monitor, or the facial verification technology may malfunction and send out false alerts that trigger an ICE ATD program violation alert (i.e., equipment tampering).[37]

Mitigation: This risk is partially mitigated. The ICE ATD program has established an alert

[37] YACMP does not use the ISAP Monitoring App or other forms of electronic monitoring technology. As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements set forth under the non-detained docket management process.

response process that the ICE ATD Servicer is required to follow in the event the assigned technology malfunctions or fails to complete a successful facial or voice match due to technology failure. Where a technology malfunction results in an "ICE ATD failure to comply alert," the ICE ATD Servicer who receives the alert initiates outreach to the ICE ATD participant to investigate the nature of the compliance failure before any law enforcement action is taken. If the ICE ATD participant does not answer a phone call from the ICE ATD Servicer, the ICE ATD Servicer will reach out to the ICE ATD participant's contacts. If it is determined that the compliance failure is due to a technology malfunction, regardless of using an ICE ATD-issued phone or personal phone, the ICE ATD participant is not penalized in any way and is provided further instructions to correct and/or replace the faulty technology.

Privacy Risk: There is a risk that information collected from noncitizens and maintained in ICE systems could contain inaccurate information about individuals participating in an ICE ATD program.

Mitigation: This risk is partially mitigated. During YACMP enrollment, information provided by the referring entity is confirmed with the YACMP participant and any additional information required for program purposes is collected directly from the YACMP participant during the orientation process. During ISAP enrollment, the information collected on Form 71-015 is confirmed with the ICE ATD participant during enrollment. Additionally, this information is compared against the ICE ATD participant's information already maintained in their Enforce Alien Removal Module case file to ensure the information is up-to-date and accurate. If the individual has never been encountered by DHS before, the ICE ATD Case Manager will create the ICE ATD participant's case file in the Enforce Alien Removal Module with information provided by the participant. ICE ATD collects biometric data directly from the ISAP ATD participant during the time of enrollment to ensure the proper voice print or face image is captured and there are no errors with the technology. Therefore, the information collected and maintained is accurate, provided the participants provided accurate responses to Form 71-015 questions.

In addition, the collection and use of information is relevant to the ICE ATD program's missions and ICE functions and is necessary to allow ICE ATD Case Managers to monitor and supervise YACMP and ISAP ATD participants, validate their identity at subsequent check-ins, and ensure the participant's compliance with an ICE ATD program. All ICE employees and contractors involved in an ICE ATD program are required to take the mandatory Annual Information Assurance Awareness Training and Privacy Training, which stress the requirements for appropriate and authorized use of information maintained in DHS information systems, including ICE ATD's case management system. ICE ATD specific user system access roles are in place to mitigate the risk of unauthorized persons accessing ICE ATD case management system. Role-based access is granted to authorized personnel with a need to know and is curtailed to their specific role duties. Finally, ICE ATD program management ensures ICE personnel have been

trained and are instructed to collect and use data only to the extent required to enroll the ICE ATD participants in their respective ICE ATD program and to monitor and supervise them while they are in an ICE ATD program. The ICE ATD Servicer is also required by its contract with ICE to only use the data to the extent necessary to fulfill their contractual duties.

7. Principle of Security

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

The information collected in the ICE ATD case management systems is stored in secure servers that only ICE ATD program personnel (i.e., contractors and ICE employees) with a need-to-know can access and view to perform tasks on their assigned ATD cases. Enforce Alien Removal Module users can read the data, but only ICE ATD Servicer personnel with the need-to-know are able to edit the data. In addition, only ICE ATD Servicer personnel operating under ISAP or YACMP have access to the associated ICE ATD case management system. As noted above, ICE is the owner of all ATD information, while the ICE ATD Servicer is the custodian of the information maintained in the ICE ATD case management systems. Finally, the ICE ATD case management systems are maintained on a secure server, meet ICE information technology requirements, and maintain Authority to Operate (ATO) in accordance with DHS and Federal Information Security Modernization Act (FISMA) standards.

Privacy Risk: There is a risk that unauthorized ICE ATD Servicer personnel or ICE personnel unaffiliated with the ATD programs could access or modify ATD information.

Mitigation: This risk is partially mitigated. Only authorized ICE ATD program personnel can access or modify the data in Enforce Alien Removal Module or in the ICE ATD case management system. The ICE ATD Servicer has in place the following security measures so that only those with the need-to-know and assigned to a case can access a particular ICE ATD participant's file:

- The ability to access or modify data in ICE ATD case management systems is restricted to select individuals in a system or database administration role. These individuals undergo background checks and are required to complete annual privacy and sensitive information training. Only upon successful completion of background checks and training are personnel allowed to access ICE information systems and ATD information.
- All logins, whether successful or unsuccessful on the ICE ATD Servicer's system, are logged for auditing purposes.

In addition, system administrators employ role-based access controls to ensure only authorized users can access information in a system that is necessary to perform their official duties. Only

those designated Enforce Alien Removal Module Standard users have read-only access to ICE ATD information. Further, only those users with the ICE ATD standard user role in Enforce Alien Removal Module can edit Enforce Alien Removal Module cases. The ICE ATD standard user role allows a user to add, edit, and delete an ICE ATD record in Enforce Alien Removal Module as well as associate supporting information. Any suspected or confirmed misuse of data, unauthorized access to a database, or inappropriate disclosure of sensitive information must be reported and handled as a privacy incident.[38] For cases of potential misconduct by ICE personnel, the incident will be reported to the ICE Office of Professional Responsibility 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 personally identifiable information, and should audit the actual use of personally identifiable information to demonstrate compliance with these principles and all applicable privacy protection requirements.

All ICE ATD personnel are required to adhere to the *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*,[39] for the collection, storage, use, dissemination, and disposal of personally identifiable information, and all other laws, regulations, and policies as Enforcement and Removal Operations employees. ICE ATD's program management ensures individuals have been trained and are instructed to collect and use information only to the extent required to enroll the participants in the ICE ATD program and monitor and supervise them while the participants are in the program. In addition, the ICE ATD Servicer is required to adhere to the terms of the Intensive Supervision Appearance Program contract with ICE to only use the data to the extent necessary to fulfill their contractual duties. All ICE ATD program personnel receive annual privacy training to ensure proper use of personally identifiable information, including the proper procedures and reporting requirements for notifying ICE of privacy incidents.

Privacy Risk: There is a risk that because the ICE ATD Servicer is a contractor, ICE personnel will not have sufficient oversight over the ICE ATD-related IT systems or ICE ATD Case Managers to ensure compliance with ICE and DHS policies and procedures.

Mitigation: This risk is mitigated. Enforcement and Removal Operations ATD Monitoring Officers or Regional Juvenile coordinators (i.e., Enforcement and Removal Operations program personnel) work with contractors on case reviews and mandatory monthly check-ins to ensure that the program is operating correctly and in compliance with privacy requirements. In addition, mandatory quarterly audits ensure that reviews and check-ins are being done correctly.

[38] *See* U.S. DEPARTMNET OF HOMELAND SECURITY, HANDBOOK FOR SAFEGAURDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (2017), *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.
[39] Id.

Enforcement and Removal Operations program personnel review and assess any emergencies and other serious events to ensure contractor compliance in how these situations are resolved. Finally, in addition to the monthly review, Enforcement and Removal Operations is forming a unit to review cases weekly as an added layer of oversight to ensure accountability.

Privacy Risk: There is a risk that the ATD Case Manager will use the location function within the Monitoring App to locate an ISAP ATD participant for non-ATD purposes or track the ATD participant's location in real-time or improperly access historical data.

Mitigation: This risk is partially mitigated. YACMP does not use the ISAP Monitoring App or other forms of electronic monitoring technology. As with all noncitizens on the non-detained docket, YACMP ATD participants' cases remain under ICE supervision and participants are required to adhere to ICE check-in requirements set forth under the non-detained docket management process.

The Monitoring App is an ISAP contractor-owned, proprietary technology and its functionality is customized for ICE's purposes to meet the ICE ATD program requirements. Unlike the global positioning system ankle monitors, the Monitoring App does not continually track the ATD participant's location. As noted above, the Monitoring App's technology is designed to only send the ATD participant's location data point—longitude and latitude coordinates—at the time the individual logs into the application and at the time of check-in. Therefore, these security features prevent the ATD Case Manager from obtaining the ATD participant's location data at any time other than what is required under the program.

In addition, the Monitoring App has a thirty minute "time-out" security measure if the ATD participant leaves the Monitoring App running in the background. After thirty minutes, the ATD participant will be required to log back into (on their own device) or open the application on an ICE-issued device. During the thirty minute "time-out" session, the Monitoring App does not continue to transmit location data; location data is only sent to the ATD Case Manager during the login in process and when the check-in is completed. Therefore, because location data is only transmitted to the ATD Case Manager during the login or check-in processes, this is the only historical data ATD Case Managers have access to, which may only be accessed to ensure compliance with ICE ATD program requirements.

Finally, alerts and notifications generated by the Monitoring App are based on conditions and parameters set by ICE Enforcement and Removal Operations. For example, an alert can be configured to send a notification to the ATD Case Manager if the ATD participant misses a check-in. Only ICE personnel have the sole authority to configure these requirements and parameters for system-generated alerts and notifications.

Conclusion

ICE administers the YACMP and ISAP ICE ATD programs to provide a cost-effective alternative to detention of eligible noncitizens who are deemed suitable for enrollment in ICE's non-detained docket. To prevent flight risk and ensure the safety and proper participation of individuals enrolled in ICE ATD programs, ICE must collect and use location data, contact information, and other information necessary to monitor such individuals. In the ISAP program, ICE utilizes tools such as ankle monitors and mobile phone applications, which collect real time data on participants. Due to the sensitivity of information collected, ICE ensures that ICE ATD participants' privacy interests and information are protected by limiting the types of information collected, applying of data safeguards, mandating training for all ICE personnel and contractors involved in the program, and maintaining compliance with applicable privacy laws and directives. Through these processes, ICE ensures that all information is collected, maintained, and used in compliance with applicable law and policy. ICE will continue to adhere to all law, regulation, and policy requirements and update this Privacy Impact Assessment accordingly.

Responsible Officials

Amber Smith
Deputy Assistant Director
Office of Information Governance and Privacy
U.S. Immigration & Customs Enforcement
Department of Homeland Security
(202) 732-3000

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Mason C. Clutter
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Appendix A - Case Management Pilot Program (CMPP)

March 17, 2023

The DHS Office for Civil Rights and Civil Liberties (CRCL) Case Management Pilot [hereinafter referred to as CMPP] is an Alternatives to Detention (ATD)[40] program launched in 2023. The ICE ATD programs described in the above Privacy Impact Assessment (PIA) are overseen and managed by the ICE Office of Enforcement and Removal Operations (ERO) and are complemented by CRCL's CMPP. Pursuant to the Department of Homeland Security Appropriations Act (2021),[41] noncitizens already enrolled in the ICE ATD programs, including the ICE Intensive Supervision Appearance Program, are able to transition their ATD enrollment to the CMPP program in the geographic locations served by CMPP.

The stated goal of CMPP is to increase support services referrals for, and to provide, undocumented noncitizens voluntary case management services[42] without the use of monitoring technology. CMPP services are provided by community-based nongovernment organizations (NGO) and/or local governments[43] through a case management services grant pilot administered by CRCL and executed by NGOs/local governments.[44]

Like ICE ATD programs, CMPP allows enrolled noncitizens age eighteen (18) and older in immigration proceedings who are not detained in an immigration facility to remain in their selected community pending the outcome of their immigration case. In accordance with ICE's legal authorities and mission, Enforcement and Removal Operations personnel enforce supervision and reporting requirements upon all ATD participants, including those whose case management services are overseen and managed by CRCL through CMPP.

---

[40] ATD consists of other distinct programs such as the U.S. Immigration and Customs Enforcement (ICE) Intensive Supervision Appearance Program (ISAP) and Young Adult Case Management Program (YACMP) ATD programs.

[41] Consolidated Appropriations Act, 2021, Pub. L. 116-260, Div. F, Title I, 134 Stat. 1182, 1449 (2020), *see also* Division F, Department of Homeland Security Appropriations Act, 2021, Joint Explanatory Statement (Joint Explanatory Statement), at 29-31, *available at* https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-F.pdf.

[42] In contrast to the above Privacy Impact Assessment, this Appendix does not use "case management services" to refer to *both* participant support services, such as the ICE ATD Extended Case Management Service and Wraparound Stabilization Services, and compliance monitoring, such as electronic monitoring. CMPP case management provides *only* participant support services.

[43] For ease of reference in this Appendix, the acronym NGO should be understood to include both nongovernmental organizations as well as local governments. This convention applies to the CMPP Enrollment Flowchart at the end of this Appendix as well.

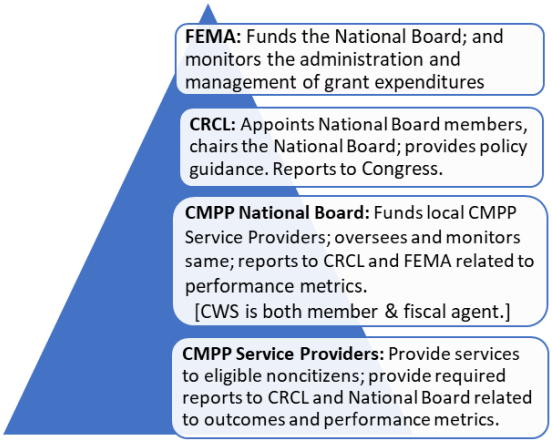
[44] NGOs and/or local governments are selected as CMPP service providers through a public solicitation process. The National Board posts a solicitation for CMPP service providers, which includes objective criteria and expectations for service providers. Applicants submit responses to the Board's solicitation within a designated timeframe and the Board selects CMPP service providers through Board vote after review and scoring of the applications. Criteria for selection included, among others, demonstrated capacity to provide voluntary and trauma informed case management services to immigrants, victims of trafficking, refugees, and/or asylum seekers, and experience with federal grant awards.

CMPP is overseen and managed by a National Board chaired by the DHS Officer for Civil Rights and Civil Liberties.[45] Additional Board member organizations include Church World Service, Catholic Charities USA, and the Center for Migration Studies of New York. Church World Service also serves as the Secretariat/Fiscal Agent for CMPP and performs necessary administrative duties for the National Board, including financial oversight of National Board subrecipients consistent with the requirements of 2 C.F.R. Part 200. On behalf of the National Board, Church World Service also provides primary management oversight of the NGO/local government's development and implementation of their CMPP privacy policies, based on requirements provided by CRCL, in consultation with the DHS Privacy Office, and the National Board.

While ICE Enforcement and Removal Operations will be fully engaged in monitoring CMPP participants' compliance with their immigration obligations, the NGO/local governments, selected by the National Board as grant subrecipients, provide services, directly or indirectly (through contracts with other service providers), in the established geographic locations. Most of the NGO/local government applicants will represent a consortia of community-based service providers and, thus, will support a whole-community approach to providing case management and other needed services to CMPP participants. Local government subrecipients may contract with community-based service providers to provide services to CMPP participants.

[45] The CMPP National Board structure is modeled on the Emergency Food and Shelter Program. See Division F, Department of Homeland Security Appropriations Act, 2021, Joint Explanatory Statement (Joint Explanatory Statement), at 29-31, *available at* https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-F.pdf. As such, funds are granted from FEMA to the National Board. The National Board is responsible for, among other things, awarding funds to qualified NGOs/local governments (subrecipients) to provide CMPP services. The baseline criteria for the Board's selection of subrecipients is outlined in the Notice of Funding Opportunity for the National Board.

CMPP Governance and Funding Structure



Eligibility for the CMPP Program

All CMPP enrollment pathways start with participation in an ICE ATD program. All individuals (including heads of household with family units[46]) eligible for ICE ATD programs are eligible for CMPP. The enrollment criteria and processes for ICE ATD programs are described in the above Privacy Impact Assessment. Specifically, absent extraordinary circumstances, noncitizens 18 years of age or older are eligible for placement into the ICE ATD programs if they currently are in removal or immigration proceedings and participation in an ICE ATD program is not prohibited by court order. Individual candidates are evaluated on a case-by-case basis before they are enrolled in an ICE ATD program.[47] In addition, CMPP candidates must be in the geographic areas served by CMPP.[48] Due to limited resources, the geographic areas for the CMPP pilot, and the need to conduct an appropriate evaluation of the program during the pilot phase, many individuals with an interest in continuing in CMPP may not be transitioned into the pilot program.[49]

CMPP Enrollment Processes

There are several pathways to CMPP enrollment. The CMPP Enrollment Pathways Flowchart depicted at the end of this Appendix provides a graphic representation of three distinct

[46] For purposes of CMPP, ICE defines a "family unit" as an adult noncitizen parent or legal guardian accompanied by their own juvenile noncitizen child(ren).
[47] As noted in the above Privacy Impact Assessment, ICE Enforcement and Removal Operations personnel consider many factors, such as age, medical status, and criminal history, when deciding if ICE ATD program enrollment is appropriate.
[48] In the initial CMPP pilot launched in 2023, the local NGO service providers will be led by the International Rescue Committee in New York, NY, and BakerRipley in Houston, TX.

but similar pathways. As noted previously, CMPP participants must first be enrolled in an ICE ATD program. Thereafter, CMPP participants can either be 1) "walk-ins" at an NGO/local government location where the individual is informed about CMPP; 2) informed about CMPP by CRCL at an ICE Field Office or other CMPP-related location; or 3) through direct outreach from CMPP. Accordingly, CMPP protocols include randomization of the names of interested individuals into two groups, only one of which will receive NGO/local government services through CMPP. Randomization supports equitable access to the limited pilot program. The CMPP pilot provides for direct transition of individuals into CMPP once ATD participation is confirmed and the appropriate consent forms have been completed.[50]

Walk-Ins

Individuals who walk-in to a participating NGO/local government office engage with a representative who describes to them CMPP. Once CMPP is described, individuals may express an interest in CMPP services or decline services. NGO/local governments collect data directly from interested potential participants. That list of interested parties is shared with CRCL, who confirms eligibility (i.e., enrollment in ICE ATD) and then randomizes the list and returns to the NGO/local government a list of individuals selected to participate in CMPP. The potential participant will then meet with the NGO/local government to enroll and sign "Consent Form A." Consent Form A allows certain core personally identifiable information (PII) to be shared with CRCL and permits CRCL to then share certain limited information with ICE for the sole purpose of removing the individual from ICE ATD programs.

ICE Field Offices or Other CMPP-Related Locations

The first interaction occurs when an individual visits an ICE Field Office, generally to handle other immigration-related requirements or responsibilities. An onsite CRCL representative informs potential participants about CMPP. Individuals may express an interest in CMPP services or decline CMPP services. CRCL then collects personally identifiable information data directly from interested potential participants, verifies the individual's participation in ICE ATD, and, after randomizing potential participants, shares the identity of a subset of the potential candidates with a participating NGO/local government. The potential participant will review and sign CRCL "Consent Form B," allowing certain information to be shared by CRCL with the NGO/local government.

[50] As cited in footnote 2, CMPP was created by statute as a DHS pilot program for the purposes of testing and evaluating the effectiveness of voluntary case management services for noncitizens in immigration removal proceedings. CMPP provides an opportunity for DHS to assess the demand for CMPP services and for nonprofit and/or local government capacity to provide and/or connect voluntary participants to effective services. DHS plans to evaluate effectiveness by looking at what, if any, impact CMPP services have on participants' attendance at immigration court hearings, compliance with immigration obligations and orders, ability to secure legal representation, and ability to access a range of social services that CMPP participants identify as priorities through an individual participatory service planning process.

Direct Outreach

ICE identifies potential CMPP candidates who are already enrolled in an ICE ATD program and provides specified personally identifiable information about the potential CMPP candidates to CRCL.[51] CRCL uses the personally identifiable information to contact the individuals to assess their interest in CMPP, either through direct CRCL outreach or through NGO/local government outreach (after CRCL has shared limited personally identifiable information with the NGO/local government for the sole purpose of contacting potential candidates for possible enrollment). Potential participants may express interest in CMPP services, decline such services, or may not be reached within the designated time.[52]

Confirmed Interest from All Enrollment Pathways

Individuals who express interest in transferring to CMPP are randomized[53] into two groups: one that will not receive services (control group) and a "services group" that will receive services. Candidates in the services groups are assigned to geographically appropriate NGO/local governments, which then verify to CRCL that an individual is enrolled in CMPP. While the NGO/local governments provide the final enrollment verification notice to CRCL, the NGO/local governments do not make independent CMPP eligibility determinations. Once CRCL (pathway 2) or the NGO/local government (pathways 1 and 3) makes the initial determination that an individual is enrolled in ATD and the individual expresses interest in transitioning to CMPP, the NGO/local government completes the final step in the overall CMPP transition process. Using the participant's A-Number, CRCL confirms the NGO/local government's initial determination of ICE ATD enrollment for each participant before names are presented to ICE Enforcement and Removal Operations for removal from ICE ATD programs.

Upon successful CMPP enrollment, CRCL notifies ICE Enforcement and Removal Operations of the individual's enrollment in CMPP, and ICE Enforcement and Removal Operations then disenrolls the CMPP participant from the services provided through and any technology monitoring under the ICE ATD program. As described below, CMPP grant subrecipients then provide case management services and make referrals for direct services and/or

[51] Individuals whose information is shared with CRCL are not directly notified of that sharing and provided an opportunity to consent or opt-out of this information sharing. However, ICE collects ICE ATD participants' personally identifiable information pursuant to its own authorities and provides notice of potential sharing through the above Privacy Impact Assessment, Privacy Act Statements, and other mechanisms.

[52] Personally identifiable information is shared in time-limited tranches to limit data retention by NGOs. DHS/CRCL, in consultation with Church World Service and the NGO/local government service provider, will set the time period for each tranche at the time the tranche is released to the NGO/local government. As part of its oversight, Church World Service will confirm to DHS/CRCL the appropriate purging of the data through required "end-of-tranche" reporting.

[53] As noted previously, randomization supports equitable access to the program and permits a robust evaluation of the program. CRCL is developing an evaluation plan for this pilot program, which will be reviewed and approved by the National Board.

upon request of the individual CMPP participants. Services may be indirectly provided through NGO/local government contracts with other service providers in the designated geographic areas. After being disenrolled from the services provided by the ICE ATD program, the CMPP participant's immigration case remains under ICE supervision and participants are required to adhere to ICE check-in requirements and all other applicable ATD requirements, except for technology monitoring. The CMPP participant is required, at a minimum, to adhere to ICE Enforcement and Removal Operations' annual check-ins and ongoing reporting obligations, although additional check-ins and oversight may be required by ICE Enforcement and Removal Operations.

Information Collected for CMPP Enrollment

In accordance with ICE and CRCL legal authorities and relevant ICE Privacy Impact Assessments and System of Records Notices (SORN), ICE Enforcement and Removal Operations will share the below core ICE ATD participant information with CRCL. ICE will also identify those individuals flagged for enhanced data protection under 8 U.S.C. § 1367 (i.e., special protected classes).

- Participant's full name;
- Mailing and physical addresses;
- Preferred language;
- Email address;
- Date of birth;
- Phone number;
- Designation as head of household (if applicable); and
- A-Number.

No new personally identifiable information is collected from individuals for participation in CMPP.

Before enrollment in CMPP**,** CRCL shares personally identifiable information (e.g., name, email and physical addresses, date of birth, preferred language, head of household designation in family unit (if applicable), and phone number) received from ICE with the CMPP NGO/local government service providers via a password-protected, organization-specific spreadsheet or other mechanism sent through the National Board's Fiscal Agent, Church World Service.[54] After CMPP

[54] Church World Service will not have access to the encrypted personally identifiable information, only to the fact of its transfer, associated deadlines, and number of individuals about whom data is being transferred. This framework

enrollment, the personally identifiable information shared with NGOs/local governments and service providers is annotated to indicate whether the individual is enrolled in CMPP, including, for participating individuals who are a head of household, the number of people in the family unit . The encrypted data results are returned by the NGO/local government and service providers through Church World Service to CRCL. ICE and CRCL will manage a protected SharePoint site to share the necessary data, as appropriate. ICE Enforcement and Removal Operations uses this information to remove newly enrolled CMPP participants from the services offered through the ICE ATD program and to verify removal. ICE Enforcement and Removal Operations will continue to monitor CMPP participants' immigration cases as they remain under ICE supervision and participants are required to adhere to ICE check-in requirements and other release conditions (e.g., court hearings, and/or check in at an ICE field office or other check-in processes). However, CMPP will not use electronic monitoring. Therefore, upon transition to CMPP, if an individual in an ICE ATD program was being monitored electronically, their ankle monitors will be removed; the Monitoring App mobile application will be removed from their personal cell phones; and ICE-issued devices with the Monitoring App mobile application will be returned. However, once enrolled, a CMPP participant's record will continue to be maintained in ICE's Enforce Alien Removal Module and tracked to ensure compliance with immigration requirements.

CMPP Case Management Services

CMPP service providers will provide case management services[55] including but not limited to:

- Mental health services;
- Human and sex trafficking screening;
- Legal orientation programs;
- Cultural orientation programs;
- Connections to social services; and
- For individuals who will be removed from the United States, reintegration services.

All CMPP participants are (by virtue of CMPP participation) able to voluntarily access all services offered by the NGO grant subrecipients.

Like the ICE ATD Extended Case Management Service and Wraparound Stabilization

is necessary to permit Church World Service to fulfill its oversight role on behalf of the National Board, while also minimizing the amount of personally identifiable information provided to NGOs/local governments s with an established need to know.

[55] If a CMPP participant requests help with the completion of a U.S. government form, the CMPP provider may provide assistance. CMPP providers will not act as agents for CMPP participants in any application for immigration benefits.

Services described in the above Privacy Impact Assessment, CMPP family units are enrolled under a head of household. The number of members in the household is identified at the time of enrollment by the NGO conducting the enrollment. The NGO then provides the number of members of the family unit when reporting back new enrollments to CRCL.

Determinations of CMPP Program Disenrollment

As part of ICE ATD, CMPP participants are bound by certain requirements and may be disenrolled from CMPP if those requirements are not followed.[56] In certain instances, after an individual is enrolled in CMPP, ICE Enforcement and Removal Operations may determine that the participant presents a risk to public safety and may decide that technology monitoring, as described in the Privacy Impact Assessment above, is required. As a result, the individual would be disenrolled from CMPP and re-enrolled in ICE ATD or potentially detained depending on the circumstances of the case. ICE Enforcement and Removal Operations exercises independent judgement to make individualized safety and risk assessments.

In the event a head of household for a family unit receiving CMPP services is no longer eligible for CMPP, the National Board will make a case-by-case decision on services continuation for the rest of the household unit. The National Board will consider the NGO/local government's recommendations and forthcoming CMPP program guidance. If a CMPP participant moves out of the CMPP geographic service area, is detained by ICE Enforcement and Removal Operations, or CMPP has made a determination that (based on ICE Enforcement and Removal Operations action) the individual no longer meets CMPP program parameters, the individual will be disenrolled from CMPP. In these instances, CMPP participant will be disenrolled without notification of their disenrollment.

CMPP Program Evaluation Purpose and Data

The CMPP pilot provides an opportunity for the Department to evaluate the effectiveness of case management services that are voluntary, overseen and managed through a National Board, and provided by community organizations. As required by the Department of Homeland Security Appropriations Act, the National Board plans to evaluate effectiveness by assessing the impact CMPP services have on participants' attendance at immigration court hearings and compliance with immigration obligations and orders. Lessons learned through implementation of the CMPP will help inform ICE ATD case practices more broadly. For evaluation purposes, NGOs will provide the National Board with de-identified data in aggregate form without personally identifiable information.

As part of the pilot evaluation, CRCL will use information from other DHS databases such

[56] DHS will develop disenrollment guidance during the pilot period based on program experience.

as the ICE Enforcement Integrated Database (EID)[57] and USCIS Central Index System (CIS).[58] This information will be combined and compared with CMPP program data to determine the effectiveness of the CMPP pilot program. For example, CRCL will compare CMPP enrollment data with immigration outcomes (for example, attending immigration court hearings, application for immigration relief, grant of immigration relief, compliance with removal orders) to determine if CMPP was effective. CRCL will work with ICE and USCIS to ensure appropriate access to data within their systems. CRCL will also use data from the Department of Justice's (DOJ) Executive Office for Immigration Review's (EOIR) Case Access System (CASE) to assist with program evaluation.[59]

Privacy Risk Assessment

Privacy Risk: There is a risk that participants may not know, or understand, the terms and conditions of participation in CMPP, or the ongoing ICE obligations, such as check-in requirements.

Mitigation: This risk is mitigated. There is a two-step process to explain CMPP to participants. CRCL or the relevant NGO/local government staff engage individuals through one of the enrollment pathways described above and in the appended CMPP Enrollment Pathways Flowchart. Using a CRCL and ICE-approved script, CMPP outreach staff explain CMPP services to individuals interested in CMPP. In enrollment pathway #1 (NGO walk-in) and enrollment pathway #2 (CRCL direct outreach), the approved explanation also includes information about the randomization process that will be undertaken before individuals are selected for enrollment. This engagement is conducted in the participant's preferred language, using, if necessary, in-person or over-the-phone interpreters. Individuals are also provided a CMPP Flyer that outlines CMPP program services.

After the list of interested individuals is randomized, those selected for enrollment are contacted by the NGO/local government case management staff and formally enrolled by the NGO/local government.

At the time of initial contact through CRCL's direct outreach (enrollment pathway #2), interested participants are given CMPP Consent Form B and the CMPP Information Sheet to sign and initial. CMPP Consent Form B describes the program's conditions, including the removal of technology monitoring, and permits sharing of data with third parties for the sole purpose of

[57] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.
[58] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM, DHS/USCIS/PIA-009 (2007 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[59] *See* EXECUTIVE OFFICE FOR IMMIGRATION REVIEW PRIVACY IMPACT ASSESSMENT FOR THE CASE ACCESS SYSTEM (2006), *available at* https://www.justice.gov/opcl/doj-privacy-impact-assessments.

conducting and reporting on CMPP activities. The associated CMPP Information Sheet describes the changes in the use of ICE Enforcement and Removal Operations technology monitoring, and outlines the ongoing ICE ATD immigration compliance requirements, including continued ICE check-ins at the direction and discretion of ICE Enforcement and Removal Operations. The CMPP Information Sheet also reaffirms the consequences of failure to comply with the CMPP participants' immigration compliance requirements, such as ICE check-in requirements and other conditions of release.

During the walk-in process and outreach process initiated by the NGO/local government (see CMPP Enrollment Pathways Flowchart for enrollment pathways #1 and #3, respectively), the NGO/local government will use a similar consent form, Consent Form A, that, once signed by the CMPP participant, will permit the sharing of limited information about the participant with CRCL, and permit CRCL to notify ICE for the sole purpose of the individual's disenrollment from the services offered by the ICE ATD program (i.e., ISAP, YACMP). Such information may include the participant's name, phone number, number of individuals in the household, if appropriate, and, if needed for identification verification purposes, date of birth and A-Number

CRCL also provides general notice of CMPP by the publication of this Privacy Impact Assessment Appendix.

Privacy Risk: There is a risk that individuals may not understand the enrollment processes for CMPP and its case management services, including sharing of their personally identifiable information with third parties.

Mitigation: This risk is mitigated. When contacted by CMPP outreach staff or NGO/local government case management staff, an individual may indicate that they are not interested in CMPP. After the individual agrees to transition into CMPP and is enrolled, all decisions to use the offered case management services are voluntary. Additionally, before sharing any needed personally identifiable information with a case management service provider, an additional consent form specific to the referral circumstance with a limited period of applicability must be reviewed and completed by the CMPP participant.

No individual information about service referrals or case management services provided to a CMPP participant is shared with CRCL or ICE. Only de-identified summary and aggregate data for program evaluation purposes will be reported to the Fiscal Agent (Church World Service) and the National Board.

Privacy Risk: There is a risk of improper sharing or use of CMPP participants' personal data.

Mitigation: This risk is mitigated. DHS uses training, access controls, and management oversight to ensure appropriate safeguards are in place for sharing and use of CMPP data by ICE, CRCL, NGOs/local governments, and service providers.

Training

All DHS CMPP personnel are required to complete (initially and annually thereafter) DHS Annual Information Assurance Awareness Training and Privacy Training, which stress the importance of appropriate and authorized use of personal data in government information systems. Additionally, all CMPP grant subrecipients are required to provide training to its CMPP-related service provider staff on the handling of personally identifiable information and implementation of their individual agency privacy policy. The training must be equal in scope to the DHS training outlined above. CRCL has also developed a CMPP Program Manual governing \the flow of CMPP information and how it must be used and safeguarded.

Access Control

As required by the CMPP Program Manual, access roles must be established to mitigate the risk of unauthorized individuals gaining access to CMPP data-sharing mechanisms with CRCL or ICE or any of the government database systems and/or information used in the CMPP program. Role-based access only is granted to authorized personnel with a need to know and is constrained to the user's specific user roles and responsibilities. Personally identifiable information used in CMPP is only shared with CMPP-designated staff and contractors who have the need to know to enable them to perform their duties under CMPP.

Management Oversight

The CMPP Administrator (a CRCL senior leader) will ensure that all staff and contractors assigned to CMPP complete the training requirements and that they are instructed to use information only to the extent required to enroll the participants in the CMPP program and to evaluate the program. Period audits (e.g., for retention of data, access of data) will also occur to ensure proper implementation of CMPP information handling requirements.

Further, only authorized CRCL or ICE Enforcement and Removal Operations program personnel will have access to the data on the SharePoint site. NGOs/local governments will not have access to this data and will receive only a limited subset of this data to conduct outreach responsibilities. CRCL will conduct a review/audit at least every six months of access to the SharePoint site to ensure the list of authorized users is up-to-date and each person who has access has received the requisite training.

CMPP NGOs/local governments will be required by the Fiscal Agent (Church World Service) to have a written data privacy policy that comports with the DHS Privacy Fair Information Practice Principles (FIPPs) and to provide training to service provider staff on the handling of personally identifiable information and implementation of their individual agency data privacy policy. CRCL will provide written privacy guidance, in coordination with the DHS Privacy Office, based on the Fair Information Practice Principles to Church World Service and the National Board for dissemination to CMPP service providers (NGOs/local governments). The NGOs/local

governments will be required to submit their privacy policies to Church World Service as a condition of the contract, and may be required to adjust and/or adopt additional privacy policy language provided by CRCL and/or the National Board Church World Service will be required to provide a copy of their privacy policy for review and approval by CRCL in consultation with the DHS Privacy Office. NGO/local government policies will address universal personally identifiable information data protection. Church World Service will monitor implementation of the privacy policies and report back to the National Board on any violations that cannot be remediated. Further, NGO's/local governments and service providers must provide notice to Church World Service within five business days of a breach, and work collaboratively with Church World Service regarding recovery, mitigation, remediation, and law enforcement involvement. Church World Services must provide to CRCL notice of a breach by the end of the business day following receipt.

Privacy Risk: There is a risk CMPP will collect more data or retain data for longer periods than necessary to complete the pilot program and assessment.

Mitigation: The risk is mitigated. CMPP does not collect any new data beyond the data already collected under the terms of enrollment in the ICE ATD programs, and only uses a subset of that data originally collected by ICE. Neither CRCL nor ICE receive information back from NGOs/local governments about the types of case management services in which specific participants voluntarily participate. DHS only receives aggregated reporting data about the types of case management or support services used by participants.

Data retention requirements will be implemented and monitored by the CRCL Records Management Officer. This includes ensuring data released to the NGOs is appropriately purged through "end-of-tranche" reporting. All data received from ICE Enforcement and Removal Operations to identify potential CMPP participants will be retained by CRCL based on the participation of the individual. For individuals who are not interested in participating in CMPP or who could not be reached during the outreach efforts, the data on the limited access SharePoint site will be deleted. For the following groups, data will be retained in the limited access SharePoint site for program evaluation purposes until five years after CRCL submits the final report to Congress after the end of the pilot: (1) individuals who expressed an interest in continuing in CMPP (whether CMPP services are provided), and (2) all individuals referred by ICE in enrollment pathway #3 (Direct Outreach pathway), whether they were selected for outreach. CRCL will conduct a technical/automatic purge periodically, and a manual audit every six months to ensure the correct data has been purged.

Privacy Risk: There is a risk that more information than necessary to complete CMPP responsibilities will be shared with NGOs/local governments and service providers.

Mitigation: This risk is mitigated. All information shared by CRCL with the CMPP grant subrecipients for outreach to determine participants' interest in CMPP or with the NGOs/local

governments for enrollment purposes is shared for the sole purpose of enrolling interested individuals in CMPP. This information is used for verification of identity. CRCL has worked with the DHS Privacy Office to determine the minimal amount of information necessary for the NGOs to conduct initial outreach and enrollment responsibilities.

Privacy Risk: There is a risk that inaccurate information will be shared with CMPP entities.

Mitigation: This risk is mitigated. CRCL and ICE will use an access limited SharePoint site to initiate the CMPP process. ICE and CRCL will share data on eligible participants outside the Department in accordance with DHS Management Directive 4300A (e.g., encryption, password-protection).[60] Initially, ICE will share data with CRCL for direct outreach. After the list is randomized, CRCL will then share potential participant information with CMPP outreach staff to contact individuals about potential enrollment in CMPP. Individuals selected for enrollment in CMPP are contacted by the NGO/local government case management staff and formally enrolled in CMPP by the NGO/local government. Enrollment status is then shared with ICE through the access-limited SharePoint site. ICE then removes individuals enrolled in CMPP from services previously provided through ICE ATD.

Privacy Risk: There is a risk that participants will not know where to go to correct their records.

Mitigation: This risk is mitigated. Each CMPP participant will be enrolled in the program by an NGO or local government that provides direct case management services as well as referrals for appropriate services as requested by the participants. Participants may correct their records with the NGO/local government with which the participant enrolled. The NGO/local government case manager will alert CRCL about any errors in records held by the Department and CRCL will update and correct those records. Federal CMPP staff are in direct communication with and conduct on-site visits of and provide technical assistance to the NGO/local government. The case manager will also ensure the integrity of its own records.

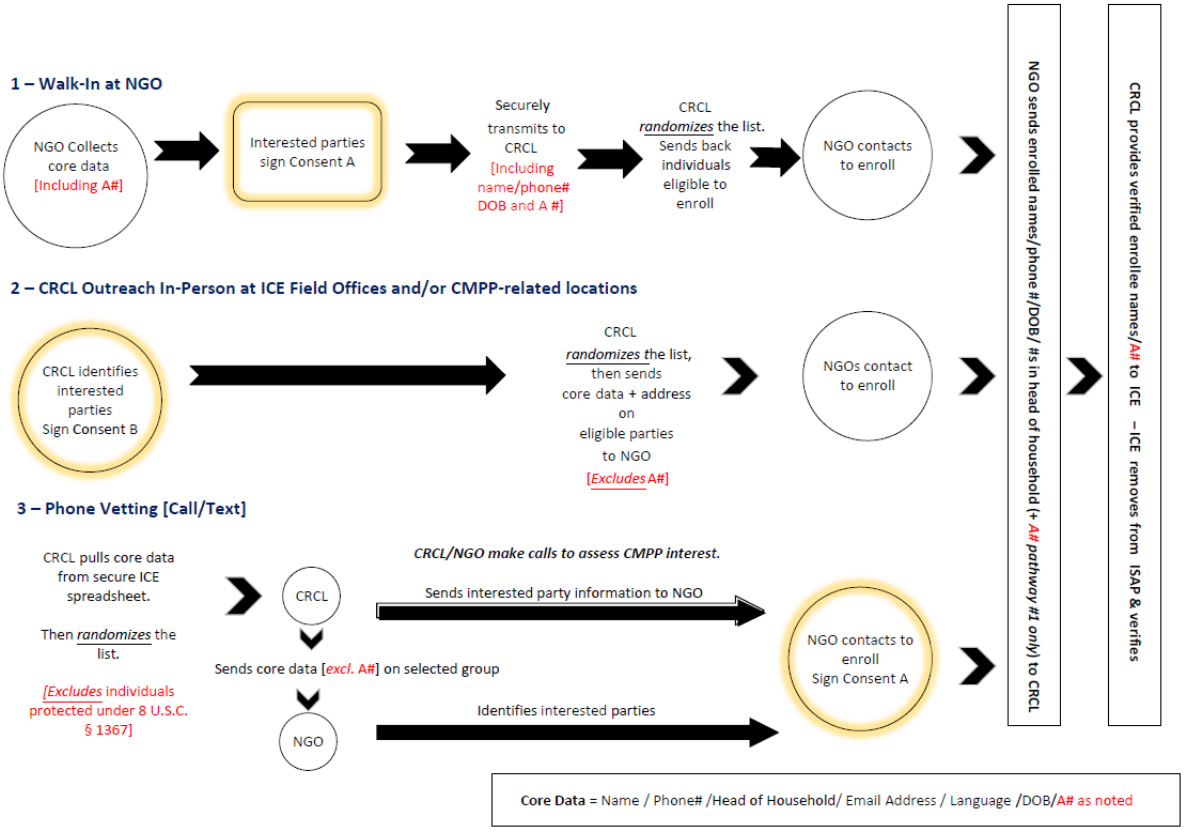
Privacy Risk: There is a risk that NGOs/local governments will not be appropriately audited and held accountable because DHS has limited oversight of the NGOs/local governments.

Mitigation: The risk is partially mitigated. Church World Service is a member of the CMPP National Board, which oversees the CMPP program. Church World Service is required to provide oversight of the NGOs/local governments' implementation of CMPP activities. This oversight includes monitoring and thorough review of required privacy documents, including policies and forms to ensure they align with CMPP requirements. Any identified concerns will be raised by Church World Service in a report to CRCL. CRCL will also provide Church World

[60] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Service with detailed privacy templates and language to use with the NGOs/local governments to ensure compliance. The CMPP National Board is chaired by the Senior Official Performing the Duties of the CRCL Officer and the Board provides management oversight of the CMPP program. Church World Service was selected to oversee the daily operations of the NGOs/local governments because of its expertise in running similar grant programs, such as the Office of Refugee Resettlement's Unaccompanied Children Post Release Services, which offers case management to minors when they are released to a sponsor in the community. Like CMPP, Church World Service held the grant with the Office of Refugee Resettlement and worked directly with affiliates that provided the case management services in that program.

CMPP Enrollment Pathways Flowchart



CMPP Contact Official

Dana Salvano-Dunn, CMPP Administrator
CRCL Director of Compliance
DHS/Office for Civil Rights and Civil Liberties
crcl.CMPP@dhs.hq.gov

CMPP Responsible Official

Peter Mina, CMPP National Board Chair
Senior Official Performing the Duties of the CRCL Officer
DHS/Office for Civil Rights and Civil Liberties