Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
(b)(6); @hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit (b)(7)(E)
If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
(b)(6); (b)(7)(C)

(b)(7)@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see (b)(7)(E) A copy of the template is available on DHS Connect at (b)(7)(E) or directly from the DHS Privacy Office via email: (b)(7)@hq.dhs.gov or phone: (b)(6); (b)(7)(C)

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
(b)(6);@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Intensive Appearance Technology Services System (IATSS) – Total Access		
Component or Office:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	Enforcement and Removal Operations, Alternatives to Detention
FISMA Name (if applicable):	IATSS	**FISMA Number (if applicable):**	ICE-08475-MAJ-08475
Type of Project or Program:	**System**	**Project or program status:**	**Operational**
Date first developed:	**January 1, 2004**	**Pilot launch date:**	**January 1, 2004**
Date of last PTA update	**August 31, 2012**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable):[1]	**In progress**	**Expected ATO/ATP/OA date (if applicable):**	**October 29, 2021**

SYSTEM OWNER

Name:	(b)(6); (b)(7)(C)		
Phone:	(b)(6); (b)(7)(C)	**Email:**	(b)(6); (b)(7)(C) @ice.dhs.gov

SECURITY ASSURANCE OFFICER (SAM)

Name:	(b)(6); (b)(7)(C)		
Phone:	(b)(6); (b)(7)(C)	**Email:**	(b)(6); @ice.dhs.gov

PROGRAM MANAGER

Name:	(b)(6); (b)(7)(C) **BI Incorporated (BI)**

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see (b)(7)(E)

Office:	Boulder, CO	**Title:**	VP, SOFTWARE SOLUTIONS/IT
Phone:	(b)(6); (b)(7)(C)	**Email:**	(b)(6); (b)(7)(C) @bi.com

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6); (b)(7)(C)		
Phone:	(b)(6); (b)(7)(C)	**Email:**	(b)(6); (b)(7)(C) @associates.ice.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA

U. S. Immigration and Customs Enforcement (ICE) is submitting this PTA renewal to complete the mandatory three-year review of the Office of Enforcement and Removal Operations (ERO), Alternatives to Detention's (ATD) Intensive Appearance Technology Services System (IATSS) (also known as Total Access). This PTA was previously submitted under the name "ERO ATD".

IATSS is a BI (i.e., contractor-owned) proprietary, cloud-based tool designed to facilitate the seamless entry, modification, and querying of data within the IATSS platform for the electronic monitoring and case management of the ATD participants (i.e., non-citizens on ICE's non-detained docket). ICE is the owner of the data generated in IATSS, while BI is the custodian. IATSS is undergoing major modification to meet ICE contractual requirements and to achieve an Authority to Operate (ATO) under the Federal Risk and Authorization Management Program (FedRAMP) with the U.S. Department of Homeland Security (DHS).

IATSS provides a holistic case management system for the ATD program, as well as electronic monitoring capabilities as needed, allowing ERO and BI staff to efficiently and securely monitor, measure, and report the case management status of program participants (e.g., court cases, check-in appointments, face-to-face visits with case managers).

BACKGROUND

The ATD program provides a cost-effective alternative to detention of non-citizens, 18 years of age or older, who are deemed suitable for enrollment in ICE's non-detained docket. ATD is a flight-mitigation program that uses technology and case management tools to ensure the ATD-enrolled non-citizens' compliance with release conditions, court hearings, and final orders of removal, while allowing them to remain in their communities as they move through the immigration process or prepare for departure from the United States. ATD is not a substitute for detention; however, it may be appropriate for non-citizens who are released pursuant to an Order of Release on Recognizance, Order of Supervision, grant of parole, or bond (unless participation in ATD is excluded as a provision). To be eligible for ATD, the non-citizens must be 18 years of age or older, effectively removable from the United States, and in some stage of the immigration process.

IATSS – TOTAL ACCESS

Case Management:

IATSS is used to keep track of the individuals through the duration of their participation in the ATD program, beginning with the initial referral into the Intensive Supervision Appearance Program (ISAP). The IATSS case management capability is used to track the participant's compliance with requirements for appearing at certain locations and/or checking in with ATD personnel, and allows BI Case Specialists to track the service options provided to them. BI personnel enter the participant's data into IATSS; ICE officers have read-only access to this information.

Service Options:

- Residential Verification
- Office Visits
- Home Visits
- Court Dates Tracking
- Community Referrals for Other Services

ISAP Electronic Monitoring:

IATSS also provides electronic monitoring functions, supporting BI's proprietary Global Positioning System (GPS) Cellular technology and Voice Verification Biometric products. Trained ATD officers determine whether the use of the GPS units are appropriate for a particpant. This technology provides the ability to verify the location information of the ATD participants being supervised, as described more fully below:

- The GPS-cellular ankle-worn products.
    - This product allows case managers and officers to establish inclusion and exclusion zones (agreed areas where the participant is, or is not, permitted to go) that can be configured by ATD personnel within the participant's area of travel through the IATSS web application. Custom alert levels and escalations are configured to notify the appropriate participant(s) regarding various events, such as the device having a low battery, or that the individual has entered an exclusion zone where he/she is not permitted to go. Events are stored in the tracking unit and delivered to the IATSS application every four hours. The device may be configured to have a higher rate of data collection and reporting, dependent upon agency needs and circumstances.
    - The program is designed to specifically monitor each subject individually. The exact GPS device, serial number, Alien Number, biographic information is directly associated with the enrolled participant assigned to each GPS device. Any alert violation related to the GPS device is sent to the assigned BI case specialist who then writes a detailed summary report and provides the report to the assigned ICE ERO Deportation Officer.
    - Each subject wearing the GPS device can be tracked in real time, by latitude and longitude coordinates, the unit's unique serial number, low battery alerts, and message delivery acknowledgements. All historical GPS points can be associated back to the subject, and can be viewed, searched and or reviewed in the Total Access system.
    - ICE case managers and officers may send a pre-programmed message (e.g., "contact your ERO officer immediately") to the GPS unit. The GPS unit will beep at regular intervals, and participants must press a button on the unit to acknowledge the message. The pre-programmed message is delivered as a recording via the unit, and participants must press the button a second time to acknowledge delivery.

- GPS data is stored within IATSS and can be retrieved by both BI and ERO designated users, who can log into Total Access and retrieve the record of the ATD participant either by name, date of birth, alien number, or EARM case number. The BI specialist or ERO officer can also view historical GPS data (e.g., point-in-time, pursuit mode) in Total Access.

- The Voice Biometric Product.
  - This product is used for identity verification and supervision purposes. The system calls the participant by phone for voice verfication at the pre-determined monthly check-in time. When the ATD participant responds, the system matches the answering individual's voice print against the pre-recorded voice in the script that the participant had created for his/her voice profile during ATD program registration.

Extended Case Management Service (ECMS):

ECMS is a component of IATSS that uses enhanced case management services to assist in stabilizing participants who may have significant vulnerabilities to ensure that they can comply with release conditions and orders issued by the Department of Justice Executive Office of Immigration Review (EOIR). Eligible participants are adult individuals and adults with non-citizen dependents or family units[2] currently in removal proceedings. Participants 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 for indigenous populations, disabilities, humanitarian, traumatic or other special vulnerabilities, as ATD personnel determines.

The family units are enrolled under a head of household. The head of household provides family member information to ECMS Case Management and Program Staff, such as names, dates of birth, alien numbers, and criminal information. Once this information is collected, Case Management and Program Staff have the ability to review cases for vulnerabilities, update or modify information based on face-to-face visits, and monitor technology and participant activities throughout the history of a participant's case.

SmartLINK Mobile Application:

The SmartLINK mobile application (app), also a BI proprietary product, was developed as an extension of IATSS. It is currently used nationally by ATD participants across the program. An ATD participant with a smartphone that meets the technical specifications of the mobile app may chose to transition off of the ATD GPS device and be monitored using the SmartLINK app.

The app allows two-way messaging and video conferencing between the participants and their BI Case Specialists. The SmartLINK app user can view his/her reporting schedule dates**.** The app requires the

[2] A "family unit" is a group of undocumented non-citizens that includes a child 17 years of age or younger who is travelling with a parent or legal guardian.

individual's location services function to be enabled so that check-in and locations of the ATD participant can be identified and recorded.

The app also has unique facial verification technology that allows for the ATD participant to register their captured facial features. A series of five photos is taken of the sujbect participant upon enrollment in ATD, using the participant's phone or the SmartLINK device. The photos are stored on a BI server. When the participant checks in, a one-to-one matching takes place against the stored profile images. The matching is automated; a case spcialist will review visually only if there is no match, or, if there is an error message. The photos are only used for the described verification purposes; ICE and BI do not share these photos with any other agency.

ERO OVERSIGHT

The ERO officers assigned to the ATD program provide management oversight of all vendors, including BI, as permitted by the contract(s) between ICE and the vendors providing services to ATD. In the case of BI, ERO ATD officers are in regular, daily contact with BI management on operational, short-term and long-term goals, and ATD field officers are in daily contact with their BI counterparts on individual cases. In addition, BI provides various reporting metrics to ERO ATD officers, as well as monthly highlights of events. See, e.g., *2108_ISAP Connections_August2021*, attached as Appendix A to this PTA.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[3] ☒ Members of the public ☐ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components): ICE employees, BI and Capgemini contractors. ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
2(a) Is information meant to be collected from or about sensitive/protected populations?	☐ No

[3] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

	☒ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[4] ☒ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

3. What specific information about individuals is collected, maintained, used, or disseminated?

The following information is collected and maintained on the non-citizen participants in the ATD program:

- Full Name
- Alias
- Alien Registration Number (A-#)
- Visa Number
- Passport Number
- Driver's License (DL) Number
- Vehicle information[5]
  - Vehicle Registration Number
  - License Plate Number
- Address
- Phone Number
- Email Address
- Date of Birth (DoB)
- Race
- Weight, Height
- Geographical Indicators (GPS)
- Employment Information
- Education Information
- Enforce Alien Removal Module (EARM) Case Number
- Name and phone number of personal contacts[6]

[4] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf.

[5] The vehicle information is not used to track participants' travel outside of their designated areas. For ATD purposes, the information is useful to inform the BI case specialist performing the home visits whether the ATD participant is at home. It is also used for law enforcement purposes(e.g., if the participant absconds and need to be located for arrest / apprehension).

[6] "Personal contacts" can be anyone the participant lists as the person BI/ERO can contact to locate the participant if he/she misses an appointment. Examples of personal contacts include (but are not limited to) attorneys, family members, friends, spouses, or legal guardians.

- Photos
- Voice record

The following information is collected and maintained on ICE employees and contractors:

- Full Name
- ICE Office Location Address
- Business Email Address
- Business Phone Numbers

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[7] If applicable, check all that apply.

☐ Social Security number ☒ Alien Number (A-Number) ☐ Tax Identification Number ☒ Visa Number ☒ Passport Number ☐ Bank Account, Credit Card, or other financial account number ☒ Driver's License/State ID Number	☐ Social Media Handle/ID ☐ Biometric identifiers *(e.g., FIN, EID)* ☒ Biometrics.[8] *Please list modalities (e.g., fingerprints, DNA, iris scans):* A photo image of the participants during check-in is compared against stored photos of the participant obtained during program registration for facial verification or confirmation. The voice of the participant responding to a call during check-in is compared against the voice print created during registration. • ☒ Other. *Please list: Click here to enter text.* Facial measurement verification software. Voice matching record; and cedula identification card[9]
3(b) Please provide the specific legal basis for the collection of SSN:	**N/A**

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

N/A

[7] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[8] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

[9] "Cedula" is a country-specific identification card. See https://en.wikipedia.org/wiki/C%C3%A9dula_de_identidad

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[10] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*
N/A

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[11] Please list all unique identifiers used: • Alien Number • EARM Case number • Phone numbers • Vehicle registration number • License plate number • Identity documents, such as: driver's license, passports, and cedula identification card • ☐ By a non-unique identifier or other means. Please describe: *Click here to enter text.*

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)**?** *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[12]	The records retention schedule is DAA-0567-2018-001-001 Participant Tracking Records, and DAA-0567-2018-0001-0002 Incident/Violation Reports. The records are destroyed seven year(s) after the cutoff date, which is the date on which the participant is terminated from the ATD Program. ERO completes a form requesting BI to terminate a participant from the ATD program. BI documents ERO's termination request in Total Access. ERO's termination request triggers an alert (a hard date

[10] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.
[11] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
[12] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/IS2O/rm/Pages/RIM-Contacts.aspx

	locked into the BI system) for BI to destroy the records seven years after the termination date. The alert prompts BI to run analytics to identify these records for destruction. Paper records at BI, if any, are manually destroyed, i.e., shredded, seven years after the cutoff date. The records in Total Access are an extension of the ICE ERO EARM system / EID. All information about the non-citizens enrolled in the ATD program that are in ICE systems fall under the EID retention schedule, which is 75 years from date of entry.
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)**?**	See response to 5 above. The records listed above with a seven-year cutoff are manually destroyed after the retention period is complete. Records in EID/EARM are automatically purged from the system according to their retention schedules.

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[13]	☐ No. ☒ Yes. If yes, please list: U.S. Citizenship and Immigration Service (USCIS) will have knowledge of the ATD participants. actively enrolled into the program in order to facilitate the asylum interview of those participants with a pending credible fear claim.
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If*	Choose an item.

[13] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

applicable, please provide agreement as an attachment.	Please describe applicable information sharing governance in place: **N/A**
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ Yes. In what format is the accounting maintained: Electronically. BI maintains the email records of the PII spill, and is required under the contract with ICE to notify ICE ERO within one hour. ICE follows the ICE reporting procedures for PII spills.

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[14] ☐ Live PII data for testing ☒ No

11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[15] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

[14] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

[15] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a government agency or program; or

(ii) the security of a government computer system.

11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
12. Does the planned effort include any interaction or intervention with human subjects[16] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[17]
13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: Privileged Users, ERO Employee Supervisors receive additional role specific privacy training.
14. Is there a FIPS 199 determination?[18]	☐ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability:

[16] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.
[17] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.
[18] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

	☐ Low ☒ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6); (b)(7)(C)
Date submitted to Component Privacy Office:	**August 24, 2021**
Concurrence from other Component Reviewers involved (if applicable):	**Courtesy copy provided to CBP Privacy**
Date submitted to DHS Privacy Office:	Click here to enter a date.

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

ERO's Alternatives to Detention (ATD) program uses technology and case management tools to increase the compliance rate of the participants with release conditions, court appearances and final orders of removal. The program allows the participants to remain in their communities as they move through immigration proceedings. ERO contracts with BI, who owns the Intensive Appearance Technology Services System (IATSS), also known as Total Access, a proprietary, cloud-based software interface that allows ATD personnel to access, update, and manage the participants' data. ICE is the owner of the data generated in IATSS, while BI is the custodian.

The records contained within IATSS are covered under the following compliance documentation:

PIAs
An ERO APP / Southwest Border Initiative PIA is forthcoming. It will cover the ATD program, including the management tools described in this PTA. In the interim, the DHS/ICE/PIA – 015 Enforcement Integrated Database PIA, and subsequent updates, b (pg 3-7, 10-13), d, i (pg. 8, 12) and j (pg 3, 5, 8), address the processes in the ATD program.

SORN
IATSS (and the ATD program) has SORN coverage under DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) 81 FR 72080 (11/18/2016), which discusses information collected to support the identification, apprehension, detention and removal of individuals unlawfully entering or present in the United States. Privacy plans to update the CARIER SORN to account for the new technologies described in this PTA that are not covered in CARIER (e.g., geo-location devices).

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6); (b)(7)(C)
DHS Privacy Office Approver (if applicable):	(b)(6); (b)(7)(C)
Workflow Number:	**0019910**
Date approved by DHS Privacy Office:	**October 7, 2021**
PTA Expiration Date	**October 7, 2022**

DESIGNATION

Privacy Sensitive System:	**Yes**
Category of System:	**System** If "other" is selected, please describe: *Click here to enter text.*
Determination:	☐ Project, Program, System in compliance with full coverage ☒ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	**New PIA is required.** Forthcoming ERO APP / Southwest Border Initiative PIA. **Interim PIA coverage:** DHS/ICE/PIA-015 Enforcement Integrated Database PIA, and subsequent updates.
SORN:	**SORN coverage to be determined** **Interim SORN coverage:** DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER).

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

ICE is submitting this PTA renewal to document the renewal of the Enforcement and Removal Operations (ERO), Alternatives to Detention's (ATD) Intensive Appearance Technology Services System (IATSS). ERO's ATD program uses technology and case management tools to increase the compliance rate of the participants with release conditions, court appearances and final orders of removal. The program allows the participants to remain in their communities as they move through immigration proceedings. ERO contracts with BI, who owns IATSS, also known as Total Access, a proprietary, cloud-based software interface that allows ATD personnel to access, update, and manage the participants' data. ICE is the owner of the data generated in IATSS.

The DHS Privacy Office (PRIV) finds that IATSS is privacy sensitive as it collects PII from members of the public and ICE employees/contractors requiring PIA/SORN coverage.

PRIV finds that a New PIA is required to provide a privacy analysis of the ATD program, including the management tools described in this PTA. PRIV agrees with ICE Privacy that interim coverage is provided by DHS/ICE/PIA-015 Enforcement Integrated Database PIA, and subsequent updates, b (pg 3-7, 10-13), d, i (pg. 8, 12) and j (pg 3, 5, 8), address the processes in the ATD program.

PRIV finds that SORN coverage is required as information is retrieved by personal identifier. PRIV finds that SORN coverage will be determined during the drafting of the forthcoming ERO APP / Southwest Border Initiative PIA. PRIV agrees with ICE Privacy that the CARIER SORN should be updated to account for the new technologies described in this PTA that are not covered in CARIER (e.g., geo-location devices).

This PTA will expire in 1 year due to the PIA/SORN requirements noted above.