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 https://www.dhs.gov/privacy-office-contacts. 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
202-343-1717

PIA@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 https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	**National Targeting Center-** (b)(7)(E)		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	NTC-Targeting Business Division
FISMA Name (if applicable):	**Automated Targeting System**	**FISMA Number (if applicable):**	**CBP-00006-MAJ-00006**
Type of Project or Program:	**New project**	**Project or program status:**	**Operational**
Date first developed:	**2021**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable):[1]	Choose an item.	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6) (b)(7)(C)		
Office:	**NTC-TBD**	**Title:**	Branch Chief
Phone:	(b)(6) (b)(7)(C)	**Email:**	(b)(6) (b)(7)(C))cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	**Email:**	Click here to enter text.

[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)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

CBP, National Targeting Center (NTC) is submitting this PTA to discuss its (b)(7)(E) Models.

The National Targeting Center (NTC), in collaboration with the Targeting and Analysis Systems Program Directorate (TASPD), builds, deploys, and maintains predictive threat rules and models at CBP's Ports of Entry (POEs) and Border Patrol checkpoints on the (b)(7)(E) to identify targets with heightened smuggling risks that may be referred for further inspection. The models leverage advanced analytics, statistical algorithms, and machine learning to target high-risk crossings in near real-time.

The Models are built from extensive research and analysis of historical seizures and crossings, derived from persistent and emerging threats related to crossing patterns and behaviors. TBD works closely with the field to gather intelligence on Drug Trafficking Organizations (DTOs) utilizing Tactics, Threats, and Patterns (TTPs) to conduct smuggling activities. The collected intelligence is researched using advanced data analytics, statistical algorithms, and machine learning techniques for determining the probability of future outcomes. The finalized model features are scenario-based, are weighted, and built into the model's architecture. The feature weight sets are based on how much a feature adds or subtracts from the risk of a seizure. Some features include time-based measurables, crossing history, high-risk relationships, and criminal affiliations.

The Models contains functionality known as threshold and suppression.

- (b)(7)(E)
-

Models identify, evaluate, and refer high-risk crossings due to a potential narcotic smuggling risk. If the crossing meets a site's set threshold and is not suppressed, the crossing is referred for secondary inspection. ATS referrals occur in conjunction with other types of system-generated referrals (CTR, TECS, NCIC, etc.) and takes precedence based on Passenger Systems Programs Directorate's (PSPDs) Hit Hierarchy listing. In secondary, an officer will receive a ATS referral with instructions for inspection; after conducting the inspection, the officer completes the closeout of a positive or negative inspection.

<u>Model Development, Refresh and Reengineering Lifecycle:</u>

The models are managed by the Land Model Environment (LME) in ATS, an electronic User Interface (UI) for managing the execution, operation, and performance of the models. Each model goes through development, refresh[2] and reengineering[3] to continually improve the model's performance and precision and to ensure old and new features are tested and evaluated. It includes an end to end iterative process and phased approach that averages around 7-10 months.

Model Example

(b)(7)(E)

Success story for model 600-

On April 15, 2021, Model 600 identified and referred a 24-year-old female U.S Citizen who attempted to smuggle narcotics into the U.S. at Deconcini, Arizona Port of Entry. The crosser was referred to secondary for additional scrutiny due to her high-risk associations, unique crossing patterns, referral history count, and weighted derogatory. At secondary, officers conducted a non-intrusive inspection (K-910 density buster) identifying anomalies in the vehicle's spare tire located in trunk. Additionally, a CBP K-9 inspection alerted to the presence of a trained odor the spare tire. A physical inspection of the spare tire lead to the discovery of 13 packages with a total weight of 14.24 kilos of fentanyl. HSI responded and federal prosecution was accepted by the AUSA. CBP seized the vehicle, narcotics, and a cellphone. Subject was transported to a federal detention facility for processing.

[2] Model Refresh is an internal process utilized by IT System Developers for retraining and re-running the development process that generated the previously selected model features, utilizing a new training data set. The model's composition (e.g., features, algorithms, hyper-parameters) remain intact; only the training data set is reinvigorated to increase the model's performance or detection elements. IT Data scientists also research seizure and crossing history since the model's deployment to identify emerging trends or behaviors aligned to the existing features that will be tested and validated for improving model performance. A Refresh is usually initiated after the Model's first six months in Production and may last up to six (6) months to complete. However, utilizing Automated Machine Learning tools, such as DataRobot dramatically accelerates the Refresh process.

[3] Model Reengineering is an internal process utilized for the redesign or restructure a model's architecture/composition and includes an overhaul of its features, algorithms, hyper-parameters that corrects degraded performance and reflect new threat research, raw intelligence or data analytics that identifies additional features aimed at improving model precision and output. This process includes acquiring updated and expanding training data sets, identifying new or changed features/attributes (evaluating the predictive benefit of each feature), and testing new model algorithms. The Reengineering process typically lasts up to nine (9) months to complete. Much like Refreshes, the incorporation of automated Machine Learning tools, such as DataRobot dramatically accelerated the Reengineering process.

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[4] ☒ Members of the public ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons While the predictive threat model is not collecting any NEW information, it does use the information in ATS on members of the public. ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ 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 ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[5] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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

[4] 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.

[5] 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*
(b)(7)(E)

The predictive threat model does not collect any additional information. The Models are scenario-based and do not use any specific criteria about individuals or vehicles. They are developed from extensive research of historical seizures, high risk crossings, and raw intelligence of persistent and emerging threats. In primary, an ATS alert will populate on the primary screen alerting the officer with instructions to refer the crossing to secondary for additional inspection. In secondary, the officer will review the posted ATS referral with instructions for inspection, complete the inspection, and post the findings.

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?[6] 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

☐ Driver's License/State ID Number

☐ Biometric identifiers *(e.g., FIN, EID)*

☐ Biometrics.[7] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.*

☐ Other. *Please list: Click here to enter text.*

The Modeling does not collect or use any of the listed information.

3(b) Please provide the specific legal basis for the collection of SSN:	*Click here to enter text.*

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.

Click here to enter text.

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*,[8] 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*

[6] 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.

[7] 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.

[8] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.

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.
Click here to enter text.

4. How does the Project, Program, or System retrieve information?	□ By a unique identifier.[9] Please list all unique identifiers used: *Click here to enter text.* □ By a non-unique identifier or other means. Please describe: N/A

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.*[10]	*The underlying information is all governed by the source system in which it was originally collected. ATS stores the underlying information for 15 years. Matches to enforcement activities or investigations will remain accessible for the life of the law enforcement matter to support that enforcement activity.*
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)**?**	***Automatic purge***

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[11]	☒ No. The models are not shared outside of CBP. □ Yes. If yes, please list:

[9] 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.

[10] *See* (b)(7)(E)

[11] 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.

	Click here to enter text.
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 applicable, please provide agreement as an attachment.*	N/A Please describe applicable information sharing governance in place: *Click here to enter text.*
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: **N/A** ☐ Yes. In what format is the accounting maintained: *Click here to enter text.*

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☒ Advanced analytics[12] ☐ Live PII data for testing ☐ No

[12] 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.

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)?[13] This does not include subject-based searches.	□ No. ☒ Yes. If yes, please elaborate: Predictive Threat Models are built from extensive research and analysis of historical seizures and crossings, derived from persistent and emerging threats. The models analyze and predict the probability of future outcomes indicative of smuggling activity.
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[14] 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.[15]

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: *Click here to enter text.*

[13] 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.

[14] 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.

[15] 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.

14. Is there a FIPS 199 determination?[16]	☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ 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:	**April 12, 2021**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	May 7, 2021

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.

(b)(5)

[16] 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.

(b)(5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
Date approved by DHS Privacy Office:	May 12, 2021
PTA Expiration Date	May 12, 2024

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:	**System covered by existing PIA** DHS/CBP/PIA-006 Automated Targeting System (ATS)
SORN:	System covered by existing SORN DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297

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

(b)(5)