Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@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 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 (b)(7)(E) 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:	**Autonomous Surveillance Towers (AST)**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	USBP PMOD
FISMA Name (if applicable):	Autonomous Surveillance Towers (CBP AST)	**FISMA Number (if applicable):**	CBP-08174-MAJ-08174
Type of Project or Program:	Program	**Project or program status:**	Development
Date first developed:	September 18, 2018	**Pilot launch date:**	June 19, 2018
Date of last PTA update	August 24, 2022	**Pilot end date:**	TBD
ATO Status (if applicable):[1]	Complete	**Expected ATO/ATP/OA date (if applicable):**	March 4, 2024

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6) (b) (7) (c), AST Program Manager		
Office:	CBP PMOD	**Title:**	AST Program Manager & System Owner
Phone:	Cell: (b) (6) (b) (7) (c)	**Email:**	(b) (6) (b) (7) (c)@cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b) (6) (b) (7) (c)		
Phone:	Cell: (b) (6) (b) (7) (c)	**Email:**	(b) (6) (b) (7) (c)@cbp.dhs.gov

[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

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP Privacy is submitting this updated PTA for the Autonomous Surveillance Towers (CBP AST). This PTA is being updated to remove the Starlink pilot from the CBP AST PTA. Starlink is not part of the CBP AST security boundary. (*See*, PTA – CBP Starlink, dated April 21, 2023). (b) (7)(E) (b) (7)(E) .
The last adjudicated CBP AST PTA is dated August 24, 2022. There has been no change to the data collected or retained by CBP AST.

Background

AST is an artificial intelligence (AI)-enabled commercially available off-the shelf (COTS) solution capable of autonomously detecting, identifying, and tracking Items of Interest (IoIs). The system is composed primarily of relocatable towers equipped with radar, camera, and onboard AI that autonomously alerts operators of potential illicit activity via a web-based user interface and mobile application.

The AST suite of sensors include (b) (7)(E) (capturing images at 1-2 frames per second), (b) (7)(E) , and a communications package mounted on a relocatable tower structure with self-sustaining power provided by an array of solar-panels and high-capacity battery packs. The AST utilize advanced computer vision algorithms to autonomously detect, identify, and track items of interest (IoI) as they transit through the towers field of view. The system can determine if an IoI is a human, animal, or vehicle without operator intervention. The system then generates and transmits an alert to operators with the location and images of the IoI for adjudication and response. If an operator decides the IoI requires a response he/she can choose to (b) (7)(E)) (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) .

The AST capture and retain imagery which occurs in plain view of the tower sites and is stored as an individual event with a unique event identifier allowing replay of the event for further investigation or dismissal based on the activity occurring. Event information (radar tracks and imagery) is stored locally at the Innovative Tower site until it synchs with the associated Amazon Web Services cloud account, established by the Office of Information Technology, where all imagery data is overwritten on a 30-day cycle. Future expansions of the pilot (b) (7)(E) (b) (7)(E) (b) (7)(E) All data is encrypted at the site and (b) (7)(E) encryption is used for all communications. The cloud environment is also hardened to encrypt the data at rest. The data utilized by the Innovative Tower is similar (radar and imagery) to other Border Surveillance Systems (BSS), such as Integrated Fixed Towers (IFT) and Remote Video Surveillance System (RVSS) covered under the DHS-CBP-PIA-022 Border Surveillance Systems (BSS). The AST only differ in the processing of the data via the application of advanced computer vision algorithms to automate the identification of an IoI instead of utilizing a USBP Agent to perform the same task. The image of an initial identification of an IoI is then distributed to USBP Agents accessing the associated browser and

mobile based applications from vendor provided devices. The USBP Agents adjudicate the image and respond, as appropriate. In the future, IoI images will be distributed to UBSP Agents via CBP issued computers, tablets and smartphones to access the vendor application. The AST will improve CBP's situational awareness and security by autonomously identifying illegal activity along the border which was previously unknown and by allowing the more efficient utilization of USBP Agents to perform border surveillance activities in the field.

The AST will be deployed to detect the presence of individuals in areas where such activity is indicative of potential illicit or illegal activity (e.g. between official Ports of Entry). CBP collects this data pursuant to its authorities under Section 103(a) of the Immigration and Nationality Act (INA or Act); Title 8, 18, 19 and 21 of the United States Code; and United States Customs and Border Protection Authorization Act H.R. 3846. The goal is to utilize this data to detect the presence – but not identify – individual(s) in an area within CBP jurisdiction.

AST – Marine Towers (August 2022)

The AST-M Towers enable remote monitoring of territory along the U.S. border for possible vessel incursions and illicit activity through the combination of towers, sensors, and computer vision algorithms. AST-M work the same way as the current surveillance towers within the AST and are currently located in the San Diego area of responsibility with possible future deployments along the Southwest Border. Besides San Diego, CBP will deploy the AST-M in the Caribbean, specifically the Puerto Rico area of responsibility; AST-M will only be deployed along coastal environments.

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[2] ☒ Members of the public In general, images are not deployed close enough to capture images from which an individual could be identified; however, in some cases PII (such as a license plate number) may be captured. ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons In general, images are not deployed close enough to capture images from which an individual could be

[2] 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.

	identified; however, in some cases PII (such as a license plate number) may be captured. ☒ DHS Employees/Contractors (list Components): In support of AST, CBP employees will have the TAK mobile application and necessary security certificates installed onto their government issued mobile device (smart phone or tablet) and will be able to share tracking and location information as well as potential threats or PoI in real-time manner. ☐ 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)[3] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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

There has been no change to the data collected or retained.

AST record imagery of border incursion activity (from a distance between (b) (7)(E) range, without facial recognition capability) allowing USBP agents to track and interdict illegal border entrants. PII of an individual beyond that of an image is not saved at the time the image is captured. Only images of confirmed detections are distributed. At this time, distributed images are provided to USBP agents accessing the associated browser and mobile based applications from vendor provided devices. Future efforts would use CBP provided desktop and mobile devices to access the vendor's application. Images are stored locally on a secured computer (physically secure and encrypted) until all events are transmitted and stored in the secure cloud storage environment. After data is backfilled to the cloud environment it is then deleted locally. All data is encrypted at the site and (b) (7)(E) encryption is used for all communications. Photographs are not retrieved by personal identifier but may be linked to PII information when associated with a prosecution case. Still images are initial evidence of an event that is not associated with any individual unless done so by a court of law during a legal proceeding. Only images associated with

[3] 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)

prosecution cases are removed from storage and associated with an individual. No information from the prosecution case is stored within the boundary of the AST Systems, only the data identified below.

Imagery Storage Information:

AST title and store each captured surveillance event by the following:

- Time and date of incursion;
- Tower camera number;
- Nearest landmark (referenced geopoint) to the event
- The type of detection: Person, Animal, Vehicle
- Image of the IoI

Image recordings are only done for law enforcement or internal training purposes. Otherwise, the imagery is not shared outside of CBP.

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?[4] If applicable, check all that apply.

☐ Social Security number	☐ Social Media Handle/ID
☐ Alien Number (A-Number)	☐ Biometric identifiers *(e.g., FIN, EID)*
☐ Tax Identification Number	☐ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.*
☐ Visa Number	☐ Other. *Please list: Click here to enter text.*
☐ Passport Number	
☐ Bank Account, Credit Card, or other financial account number	
☐ Driver's License/State ID Number	

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

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*,[6] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or

[4] 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.

[5] 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.

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

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.[7] Please list all unique identifiers used: *Click here to enter text.* ☒ By a non-unique identifier or other means. Please describe: (b) (7)(E) Information related to individuals or suspects obtained from TAK devices is not retrieved by identifier and does not require SORN coverage. In the event that TAK information is later linked to an individual subject to a CBP law enforcement event or other investigation the information would be covered by DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601.
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.*	The non-evidentiary records captured by AST will be maintained according to the Border Surveillance Systems (BSS) records schedule (DAA-0568-2018-0002). All evidentiary records captured by AST will be preserved with the associated case file and maintained for the duration of the court case. AST will also be maintaining machine learning training data, these records should not be deleted. CBP RIM (Records and Information Management)

[7] 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.

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.[8]	will work with the project teams, system owners, Privacy, and Chief Counsel to create records schedule that will be submitted to NARA for approval.
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)**?**	Technical/Automatic Purge

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[9]	☒ No. ☐ Yes. If yes, please list:
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: Surveillance images may be requested from USBP as evidence for investigations and prosecutions.
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.*	Choose an item. 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: 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[10]

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

[9] 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.

[10] 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.

	☐ 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)?[11] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
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[12] 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.[13]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual	☐ No. ☒ Yes. If yes, please list: Image recordings are only done for law enforcement or internal training

[11] 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.

[12] 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.

[13] 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.

privacy training required of all DHS personnel?	purposes. Otherwise, the imagery is not shared outside of CBP.

14. Is there a FIPS 199 determination?[14]	☐ 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

[14] 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.

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:	***May 2, 2023***
Concurrence from other Component Reviewers involved (if applicable):	*Click here to enter text.*
Date submitted to DHS Privacy Office:	*May 2, 2023*

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)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

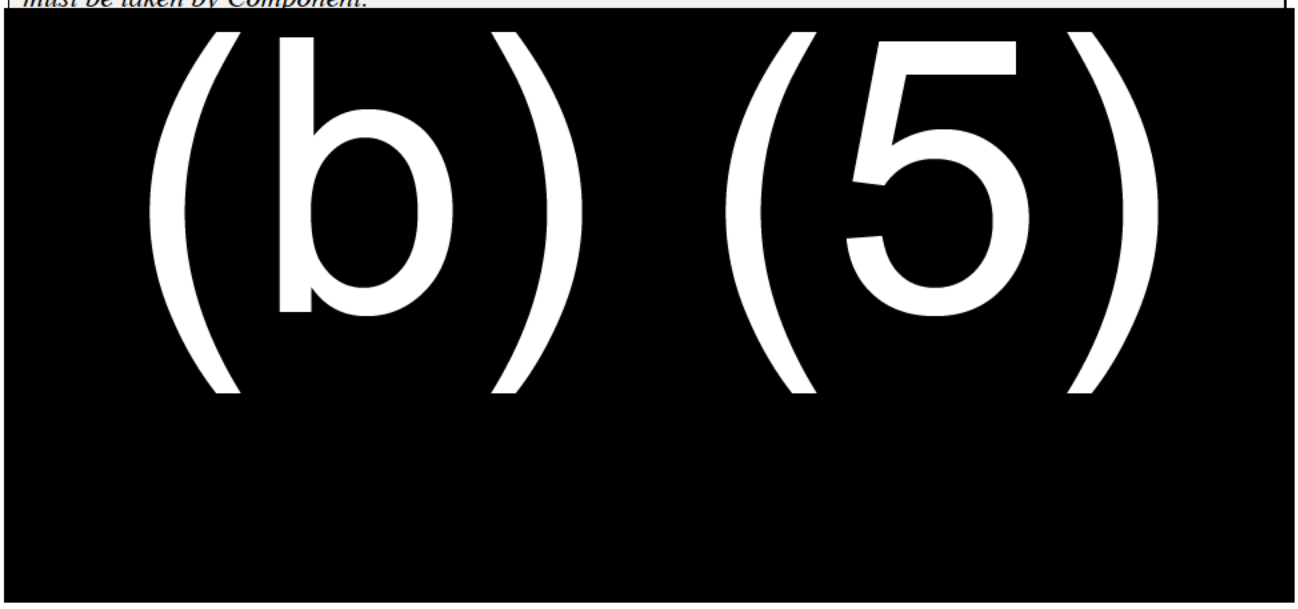
DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	(b) (6)
Workflow Number:	**0014389**

Date approved by DHS Privacy Office:	May 31, 2023
PTA Expiration Date	May 31, 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:	**PIA update is required.** • DHS/CBP/PIA-022 Border Surveillance Systems (BSS)
SORN:	**SORN coverage to be determined** • DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601

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)