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:	**Saildrone**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	Air and Marine Operations
FISMA Name (if applicable):	**N/A**	**FISMA Number (if applicable):**	**N/A**
Type of Project or Program:	**Pilot**	**Project or program status:**	**Pilot**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	**October 3, 2022**
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	**July 31, 2024**
ATO Status (if applicable):[1]	**N/A**	**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:	CBP Innovation	**Title:**	Assistant Chief
Phone:	(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:	(b) (6) (b) (7) (c)	**Email:**	(b) (6) (b) (7) (c)@associates.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

(b)(7)(E)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP Privacy is submitting this updated PTA for Saildrone on behalf of the CBP Innovation team (INVNT) and Air and Marine Operations (AMO) to extend the pilot for an additional (b) (7)(E) In addition, CBP will continue to pilot Saildrone, an autonomous marine surface vessel off the coast of (b) (7)(E) **An updated PTA will be submitted to deploying beyond this pilot period or in an operational environment.**

Overview

CBP will enter into an additional 90-day pay per service contract to pilot Saildrone in the maritime environment off the coast of (b) (7)(E). Saildrone machines are (b)(7)(E) vessels that autonomously monitor maritime environments. The vessels are equipped with a variety of sensors that capture their surroundings. The Saildrone vessel captures the following data during deployment:

- (b)(7)(E)

Saildrone vessels will be piloted to monitor the ocean for (b) (7)(E) using (b)(7)(E) to recognize, sort, and identify items of interest (IoI).

(b) (4), (b) (7)(E)

While Saildrone vessels can operate (b) (4), (b) (7)(E)

To ensure safe operations, the Saildrone is equipped with (b) (4)

(b) (4), (b) (7)(E)

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 ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☐ 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)[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, maintained, used, or disseminated.

No specific information about individuals is meant to be collected. However, the Saildrone (b) (4)

The following information will be collected, used, and retained during the pilot:

- (b)(7)(E)
-

[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.

[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)

(b)(7)(E)

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

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

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

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 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*

[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, 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: ☒ By a non-unique identifier or other means. Please describe: (b)(7)(E) [redacted]

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.*[8]	(b) (7)(E) [redacted]
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 from date of ingestion**

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: *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:

[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.

[8] *Se* [redacted] (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.

	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[10] ☐ 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,	☒ No.

[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.

[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.

aggregated, or otherwise privacy-protected?	☐ 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 privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*

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

[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.

[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:	**July 5, 2023**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	July 10, 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:	**0014830**
Date approved by DHS Privacy Office:	**July 10, 2023**
PTA Expiration Date	**July 31, 2024**

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Pilot 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-022 Border Surveillance Systems
SORN:	Choose an item. *Click here to enter text.*

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)

(b) (5)