



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:	Clarifai Software		
Component or Office:	Customs and Border Protection (CBP)	Office or Program:	Artificial Intelligence (AI) Center of Innovation (COI) Office of Field Operations (OFO)
FISMA Name (if applicable):	Click here to enter text.	FISMA Number (if applicable):	Click here to enter text.
Type of Project or Program:	Pilot	Project or program status:	Pilot
Date first developed:	October 30, 2019	Pilot launch date:	November 1, 2022
Date of last PTA update	April 25, 2023	Pilot end date:	September 30, 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:	Office of the Assistant Commissioner	Title:	Chief Technology Officer
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)@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 Office of the Commissioner, Office of Information Technology (OIT), and CBP Innovation Team (INVNT) is submitting this PTA update to extend the pilot to 9/30/24. There are no other changes to the collection, use, maintenance, and disclosure of PII.

Background

CBP Office of the Commissioner, Office of Information Technology (OIT), and CBP Innovation Team (INVNT) is piloting the Clarifai Software. Clarifai is a training data platform that will assist CBP in [REDACTED]

The Clarifai software will enable CBP to [REDACTED] (b)(7)(E) within the bounds of the CBP network and while providing an AI (Artificial Intelligence) lifecycle to deploy, maintain, and manage AI models. Using the pre-trained or custom models allows Clarifai to recognize new topics and can be used to test model performance for each new model version that is created. It can review streaming video, pre-recorded video, or image data providing the ability to use deep trained [REDACTED] (b)(7)(E)

(b)(7)(E)

CBP Use

CBP collects an incredible volume of imagery as part of its mission. CBP employees are responsible for identifying anomalies, threats, and other mission critical information based on those images. Monitoring imagery for specific objects is a highly fatiguing task, and in most cases is better suited for computers than humans. (b) (7)(E)

CBP Office of Field Operations (OFO) will provide (b) (7)(E) [REDACTED]. Only CBP will have access to the data within the Clarifai application. CBP has provisioned 10 accounts for cleared individuals within Claifai. Both the [REDACTED] will be retained by Clarifai until all proof of concepts are completed. Once the proof of concepts are completed, data will be deleted through a manual process. CBP data owners will be informed following deletion of the data within the Clarifai platform.

Authorized CBP users will log into the Clarifai software and upload select CBP data to be used in these data annotation activities and establish labeled data sets for use by CBP's Artificial Intelligence (AI) applications. Once uploaded to Clarifai, the Clarifai software will process the data and the data will be retrieved and reviewed. The annotated data will be downloaded, indexed, and stored in the CBP curated annotated data library to reside within CBP Enterprise Cloud Infrastructure (CECI) cloud security boundary, providing CBP data scientists and other relevant personnel the ability to quickly search and



collate the data for specific use cases using natural language.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)



<p>2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This project does not collect, collect, maintain, use, or disseminate any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p style="padding-left: 40px;"><input checked="" type="checkbox"/> U.S. Persons (U.S. citizens or lawful permanent residents)</p> <p style="padding-left: 40px;"><input checked="" type="checkbox"/> Non-U.S. Persons</p> <p><input checked="" type="checkbox"/> DHS Employees/Contractors (list Components): CBP</p> <p><input type="checkbox"/> Other federal employees or contractors (list agencies): <i>Click here to enter text.</i></p>
<p>2(a) Is information meant to be collected from or about sensitive/protected populations?</p>	<p><input checked="" type="checkbox"/> No</p> <p><input type="checkbox"/> 8 USC § 1367 protected individuals (e.g., T, U, VAWA)³</p> <p><input type="checkbox"/> Refugees/Asylees</p> <p><input type="checkbox"/> Other. Please list: <i>Click here to enter text.</i></p>

<p>3. What specific information about individuals is collected, maintained, used, or disseminated?</p>
<p>CBP collects imagery from a wide spectrum of sources each of which is documented in existing privacy documentation and appropriate systems documentation (ex. PTAs, PIAs, and SORNs). Examples include, but are not limited to:</p> <ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]

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

[REDACTED] (b)(7)(E)



<ul style="list-style-type: none"> • (b) (7)(E) [REDACTED] <p>With the exception of NIL, (b) (7)(E) [REDACTED]</p> <p>[REDACTED] Data is retained in accordance with each systems' published requirements for imagery and video storage.</p> <p>Clarifai captures the following user information for account creation:</p> <ul style="list-style-type: none"> • User Email (CBP email account) • User Password 	
<p>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.</p>	
<input type="checkbox"/> Social Security number <input type="checkbox"/> Alien Number (A-Number) <input type="checkbox"/> Tax Identification Number <input type="checkbox"/> Visa Number <input type="checkbox"/> Passport Number <input type="checkbox"/> Bank Account, Credit Card, or other financial account number	<input type="checkbox"/> Social Media Handle/ID <input type="checkbox"/> Driver's License/State ID Number <input type="checkbox"/> Biometric identifiers (e.g., FIN, EID) <input type="checkbox"/> Biometrics. ⁵ Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text. <input type="checkbox"/> Other. Please list: Click here to enter text.
<p>3(b) Please provide the specific legal basis for the collection of SSN:</p>	N/A
<p>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.</p>	
N/A	
<p>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</p>	

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>.



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.⁷ Please list all unique identifiers used:
Click here to enter text.

By a non-unique identifier or other means. Please describe:
Primarily by filename but can also be retrieved based on date metadata (e.g., date created, date uploaded).

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

GRS 3.1, item 11. 5 years after the CBP system or record is no longer in use

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)?

Manual Audit

6. Does this Project, Program, or System connect, receive, or share PII with any

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 See (b)(7)(E)



other DHS/Component projects, programs, or systems? ⁹	Will be collecting Data to use with Clarifai that may contain facial, license plates, or other identifiable imagery from CBP.
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i>
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:
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: CBP will follow up with Clarifai at the completion of the pilot to ensure that the CBP data is deleted. <input type="checkbox"/> Yes. In what format is the accounting maintained: <i>Click here to enter text.</i>
10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	<input type="checkbox"/> Social Media <input checked="" type="checkbox"/> Advanced analytics ¹⁰ <input type="checkbox"/> Live PII data for testing <input type="checkbox"/> No

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.



<p>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.</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i></p>
<p>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?</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i></p>
<p>12. Does the planned effort include any interaction or intervention with human subjects¹² via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort.¹³</p>
<p>13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?</p>	<p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i></p>

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/capo> 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?¹⁴	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6) (b) (7) (c)
PRIVCATS ID Number:	0015459
Date submitted to Component Privacy Office:	September 18, 2023
Concurrence from other Component Reviewers involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	September 25, 2023
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.</i>	
(b) (5)	

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. For more information, see <https://www.nist.gov/itl/fips-general-information>.



(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	Click here to enter text.
PRIVCATS ID Number:	0015459
Date adjudicated by DHS Privacy Office:	September 26, 2023
PTA Expiration Date:	September 30, 2024

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Pilot If "other" is selected, please describe: <i>Click here to enter text.</i>
Determination:	<input checked="" type="checkbox"/> Project, Program, System in compliance with full coverage. <input type="checkbox"/> Project, Program, System in compliance with interim coverage. <input type="checkbox"/> Project, Program, System in compliance until changes implemented. <input type="checkbox"/> Project, Program, System not in compliance.
PIA:	System covered by existing PIA DHS/CBP/PIA-017 Non-Intrusive Inspection Systems Program; DHS/CBP/PIA-022 Border Surveillance Systems
SORN:	System covered by existing SORN DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792
DHS Privacy Office Comments:	<i>Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.</i>

(b) (5)



**Homeland
Security**

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
Version number: 07-2023
Page 12 of 12

(b) (5)