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:	Intelligence Reporting System-Next Generation External Users		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	National Targeting Center
FISMA Name (if applicable):	Automated Targeting System	**FISMA Number (if applicable):**	CBP-00006-MAJ-00006
Type of Project or Program:	**Program**	**Project or program status:**	**Existing**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	**October 1, 2015**
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]	**In progress**	**Expected ATO/ATP/OA date (if applicable):**	

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6) (b)(7)(C)		
Office:	National Targeting Center	**Title:**	Watch Commander
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:		**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: New PTA

The Intelligence Report System-Next Generation (IRS-NG) is a web-based system developed on the Automated Targeting System (ATS) Unified Passenger (UPAX) platform that searches data sources within ATS, based on user permission. IRS-NG is used to standardize and consolidate reporting to enhance DHS' ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and to improve border security through the sharing of Informational and Intelligence Products. Previously, the creation of informational and intelligence products was inefficient and duplicative due to the inability to collaborate in a centralized, secure environment. IRS-NG mitigates these gaps and standardizes the reporting process by providing a collaborative workspace for authorized users to collect, analyze and share data, as well as create Intelligence and Informational products in a secure environment.

IRS-NG is designed to streamline the: 1) authoring of Intelligence Products, 2) optimize the use of existing data sources, and 3) promote collaboration and information sharing in a secure environment. More specifically, IRS retrieves data from searches maintained in other systems, including information from both government owned sources (see question 5) and commercial data aggregators. The reporting process is streamlined with the implementation of a collaborative workspace that enables an analyst to collect, analyze, and report on structured data and unstructured data. Providing these functionalities reduces duplication of reports with various formats generated from the same information. Simultaneously, the collaborative workspace allows analysts to search, add to, and share information. The information/intelligence products are stored within IRS-NG and then transitioned into the Analytical Framework for Intelligence (AFI) System where other permitted agencies can view the finished informational and intelligence products.

CBP is providing this PTA to give an overview of how external users request access, the requirements, and what level of accesses external users can have in the IRS-NG system.

CBP considers requests from users outside of CBP (DHS) to access IRS-NG on a case-by-case basis. External users are generally co-located with CBP working closely on joint programs. These joint programs facilitate and improve information sharing capabilities for CBP. Other government agency employees must have a valid Tier 5 Background Investigation required for all CBP system access and justify their need for access and agree to CBP's terms as outlined in the MOU/MOA regarding the proper use, handling and dissemination of data. Designated Points of Contact are responsible for updating CBP on their employees' status regarding a continued need for access. CBP also conducts regular audits on the continued need for IRS-NG access and Tier 5 Background Investigation expiration dates; and access is removed as necessary.

IRS-NG users outside of CBP will be granted the Author/Reviewer roles to create intel products, while select members, in a supervisory capacity, will be granted Supervisor Roles to publish finished products all within their designated agency's provisioned Port/Unit. These users will be selected and monitored by CBP.
Outside users will not be granted access to IRS-NG tools including the photo array feature, SaAW, Grupo Conjunto Inteligencia Fronteriza (GCIF), Threat Network Exploitation Tool (TNET), and Field Leads and Observation Workflow application (FLOW).

Roles and Permissions for IRS-NG users include:

- Consumer: Read only permissions, provisioned to their Port/Unit.
- Author: Within their provisioned Port/Unit, the Author role allows you to view data, create and populate reports, modify or delete their own reports, change the workflow status of their own reports, and submit reports for review.
- Co-Author: Within their provisioned Port/Unit, the Co-Author role allows you to view data and modify their reports.
- Reviewer: Within their provisioned Port/Unit, the Reviewer role allows you to review reports and recommend.
- Supervisor: Within their provisioned Port/Unit, the Supervisor role allows you to view data, create and populate reports, modify or delete any reports, change the workflow status of any reports, submit the report for review, review submitted reports and recommend, and approve reports that submitted by others.

IRS-NG users outside of CBP include:

- (b)(7)(E)
-
-

- (b)(7)(E)
- (b)(7)(E)
- (b) (7)(E)

Separate PTAs are conducted for every new external user request and will detail which user role that office will obtain.

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.*

[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.

	☐ 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 is no change to the IRS-NG system to the way information about individuals is collected or generated.	
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	☐ 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):* **Photos** ☐ Other. *Please list:*
3(b) Please provide the specific legal basis for the collection of SSN:	Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the

[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)

[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.

	Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108- 458, 118 Stat. 3638); The Tariff Act of 1930, as amended; The Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); The Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104- 132, 110 Stat. 1214); SAFE Port Act of 2006 (Pub. L. 109-347); Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); 6 U.S.C. § 202.

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.

SSNs are ingested or included as personal identifiers from the source systems and rely upon their authority to collect them for law enforcement and/or intelligence purposes.

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 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.*

SSNs are ingested or included as personal identifiers from the source systems and rely upon their authority to collect them for law enforcement and/or intelligence purposes.

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[7] Please list all unique identifiers used: external users can search by unique identifier. ☐ By a non-unique identifier or other means. Please describe

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

[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.

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]	CBP maintains records in IRS-NG consistent with the DHS NI-563-07-016 records schedule of the DHS Office of Intelligence and Analysis for Raw Reporting Files and Finished Intelligence Case Files.
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: Information is stored within IRS-NG workspaces, and can be added to intelligence or informational products which are published to Analytical Framework for Intelligence (AFI) System for consumption by permitted agencies/users who view the finished informational and intelligence products.
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:

[8] *See* [redacted]

[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.

	External Users outside of CBP may have access to IRS-NG and the reports published from IRS-NG to AFI.
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.*	Existing Please describe applicable information sharing governance in place: Agreements are in place with an individual working on behalf of CBP with access to CBP systems such as IRS-NG, and agencies outside of CBP that have access to IRS-NG will be memorialized in an agreement.
9. Does the Project, Program, or System have a mechanism to track external disclosures of an individual's PII?	☐ No. What steps will be taken to develop and maintain the accounting: *Click here to enter text.* ☒ Yes. In what format is the accounting maintained: The audit trails within ATS are maintained at the application levels and the database levels. The audits of who (user), what (activities) and when (date and time) are maintained in ATS for user provisioning, user logins, and user activities In addition, DHS/CBP policy require individuals fill out a DHS 191 for disclosures of information outside of DHS.

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

[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. 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.
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:

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 <u>research purposes</u>	☒ No. ☐ 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]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in</u>	☐ No. ☒ Yes. If yes, please list: All employees receive annual privacy awareness training as

[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.

addition to annual privacy training required of all DHS personnel?	well as system-specific and role-based training that covers security, privacy, and information handling requirements.

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

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6) (b)(7)(C)
PRIVCATS ID Number:	**0017523**
Date submitted to Component Privacy Office:	**July 9, 2024**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	July 11, 2024

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)

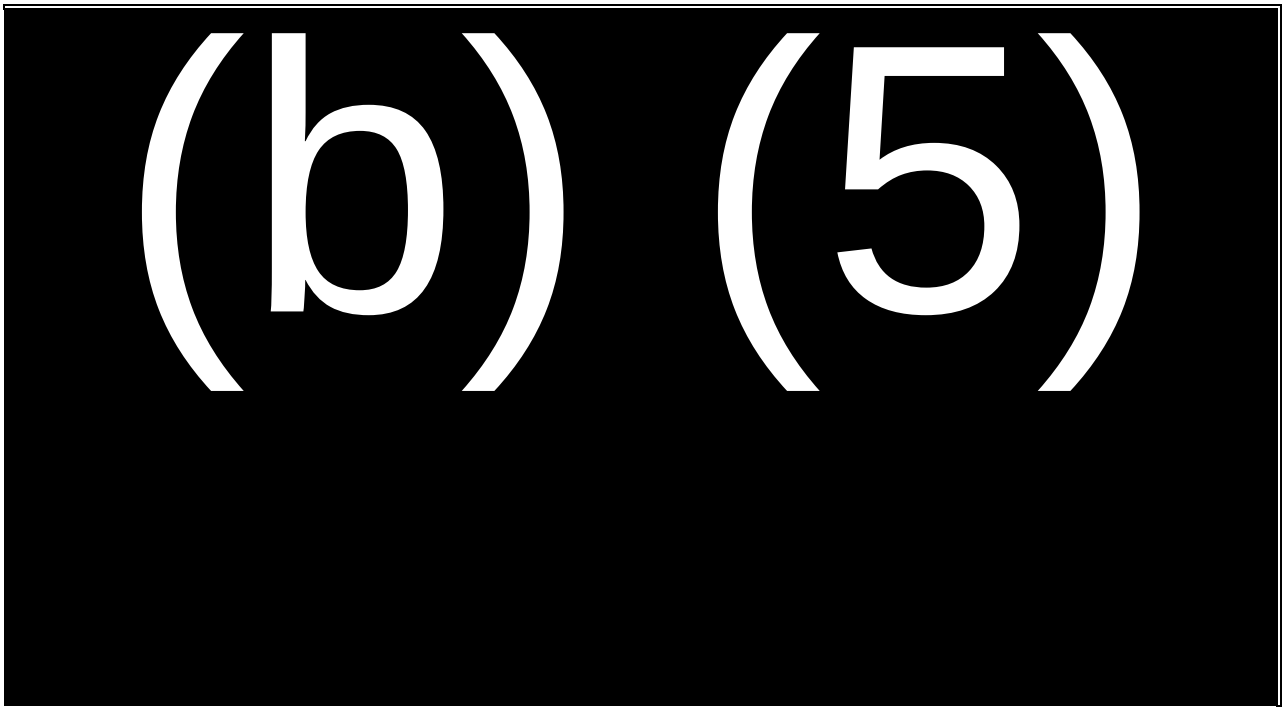
DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	(b) (6)
PRIVCATS ID Number:	**0017523**
Date adjudicated by DHS Privacy Office:	July 17, 2024
PTA Expiration Date:	July 17, 2025

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Program 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.** DHS/CBP/PIA-XXX IRS-NG – **Forthcoming**
SORN:	**System covered by existing SORN** DHS/CBP-024 Intelligence Records System (CIRS) System of Records, December 14, 2020, 85 FR 80806

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)