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:	**Seamless Integrated communication (SIC)**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	**USBP-PMOD**
FISMA Name (if applicable):	**Seamless Integrated communication (SIC)**	**FISMA Number (if applicable):**	**CBP-08910-MAJ-08910**
Type of Project or Program:	**Program**	**Project or program status:**	**Existing**
Date first developed:	**April 27, 2020**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**N/A**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable):[1]	**In progress**	**Expected ATO/ATP/OA date (if applicable):**	**April 26, 2024**

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6), (b) (7)(C) [redacted]		
Office:	**PMOD/C3/ADVON**	**Title:**	**System Owner**
Phone:	(b) (6), (b) (7)(C) [redacted]	**Email:**	(b) (6), (b) (7)(C) [redacted] @cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b) (6), (b) (7)(C) [redacted]		
Phone:	(b) (6), (b) (7)(C) [redacted]	**Email:**	(b) (6), (b) (7)(C) [redacted] @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) [redacted]

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

CBP Privacy is submitting this new PTA as part of the three-year Authority to Operate (ATO) process. Seamless Integrated Communications (SIC) is a new major FISMA system [CBP-08910-MAJ-08910]. The goal of SIC is to uniquely integrate and deploy formerly separate demonstration projects and capabilities (i.e., Hybrid Communications, Starlink, SNAP, Silvus) under one program and security boundary for the purposes and use cases described. **This PTA for operational use aligns with the SIC security boundary to include the following integrated equipment components uniquely configured to support the intent of the SIC program and capabilities:**

- goTenna
- Starlink
- Simple Network Access Point (SNAP) Kit and SNAP Cloud Service Router (CSR)
- Silvus Technologies

The use of aforementioned equipment as described under, SIC does not infer nor inherit PTA outcomes that may use the same technology elements in different applications or uses case across other CBP projects, programs or tests.

No data is stored in the SIC network as it serves only as a communications network. Data in transit is encrypted using Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) version 1.2.

<u>Overview</u>

Seamless Integrated Communications (SIC) is a system that provides enhanced situational awareness to CBP agents operating in (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E)

(b) (7)(E) is provided through multi-hop mesh radios and antennas network consisting of, Silvus MANET radios, GoTenna Pro-X antennas, backhauled through SNAP, using SpaceX Starlink ground terminal, Field Site CBP Fiber or cellular LTE services, thus improving situational awareness for up to (b)(7) end-users at any given time. SIC is critical in supporting CBP operations, CBP agent safety, providing continuous communication capability (b) (7)(E), and provide critical real-time (b) (7)(E) connected to this network.

<u>Use Cases:</u>

1. Fixed location application leverage spoke and hub model where (b) (7)(E) is routed to CBP agents operating in the field. The Starlink base station connected via ethernet to SNAP will receive and transmit (b) (7)(E). Several communication devices are integrated to create a mesh and Mobile Ad hoc Network (MANET) ensuring that (b) (7)(E) (b) (7)(E) (ex. GoTenna/Silvus (b) (7)(E)] via SNAP and Starlink).

2. Mobile application providing MANET type topology in terms of various (b) (7)(E), (b) (7)(E) (GoTenna/Silvus (b) (7)(E)] via SNAP and LTE).

The use cases above require necessary bandwidth and network access for uninterrupted communications from mobile nodes to field operators both within the CBP Amazon Web Services (AWS) Cloud East (CACE)(b) (7)(E). This data flow increases CBP's operational awareness and facilitates operator ability to interdict illicit activity. The unique requirements for security, spectrum and testing of SIC RF networks and allowed data types (b) (7)(E) (b) (7)(E)) are described and shown in the security boundary diagram (Fig. 1).

Hardware Components:

The following hardware components encompass the SIC multi-hop mesh radios and backhaul network:

Starlink Satellite

Starlink satellite terminals offer a CBP TRM approved access to commercial low earth orbit satellite constellation for high bandwidth, high availability connectivity solutions (b) (7)(E) (b) (7)(E). SIC will use Starlink as a backhaul method to (b) (7)(E) to CBP agents/officers and as a facility network enhancement where CBP fiber does not have available access or bandwidth. This provides alternatives to Long-Term Evolution (LTE), and other commercial cellular options. Connectivity will be used to (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) The intent is to utilize the capacity of each Starlink terminal to handle the backhaul load of (b) (7)(E).

Simple Network Access Point (SNAP)

The Syzygy SNAP kit is a CBP TRM approved terrestrial network access point that (b) (7)(E) (b) (7)(E) (b) (7)(E) The SNAP CSR provides for the virtual secure routing of SIC data to/from CBP Enterprise. SNAP is also fully configurable to have network failover to multiple cellular networks if the Starlink or CBP LAN networks connections drop or are interrupted for any reason. SNAP provides CBP agents with the ability to bridge communications, (b) (7)(E) (b) (7)(E).

SIC Silvus Technologies Radio

(b)(7)(E)

SIC GoTenna Portable Radio

(b)(7)(E)

Fig. 1 - Seamless Integrated Communications (SIC) security boundary diagram is shown below:

(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

[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.

	☐ 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?

No PII is collected, generated, or retained by the Seamless Integrated Communications (SIC) network. All data is passed through with encryption in place and stored in the respective CBP system of record (b) (7)(E) servers).

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): Click here to enter text.*

[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.

	☐ 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 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: N/A ☐ 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.*	**SIC does not collect or store any data. All data is transmitted and retained per the respective CBP system of record (i.e., (b) (7)(E))**

[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.

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]	
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)?	**N/A**

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: N/A
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

[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.

	☒ 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 <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 addition</u> to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*

[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]	☐ 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:	Click here to enter text.
Date submitted to Component Privacy Office:	**October 19, 2023**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	October 25, 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):	Click here to enter text.
PRIVCATS ID Number:	**0015677**
Date adjudicated by DHS Privacy Office:	October 25, 2023
PTA Expiration Date:	October 25, 2026

DESIGNATION

Privacy Sensitive System:	No
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:	Choose an item. *Click here to enter text.*
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)