



Privacy Threshold Analysis

Version number: 06-2020

Page 1 of 11

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:	NII – Underwater Inspection System		
Component or Office:	Customs and Border Protection (CBP)	Office or Program:	Office of Field Operations (OFO)/Non-Intrusive Inspection Division (NIID)
FISMA Name (if applicable):	NII	FISMA Number (if applicable):	CBP-03627-GSS-03627
Type of Project or Program:	Program	Project or program status:	Operational
Date first developed:	Click here to enter a date.	Pilot launch date:	January 1, 2022
Date of last PTA update	Click here to enter a date.	Pilot end date:	July 31, 2022
ATO Status (if applicable):¹	Choose an item.	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:	Air and Marine Operations	Title:	SMIA
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



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

CBP Privacy is submitting this new PTA to provide coverage and transparency for CBP's technology demonstration of a NII – Underwater Inspection System (UIS). CBP agent/officer will demo the NII-UIS to create underwater sonar images of the hulls of vessels and structures to detect the presence of parasitic devices (See Figure 1 for examples). Parasitic devices are anything attached to the hull magnetically or attached in some other way which may contain narcotics, firearms, money, or weapons of mass destruction. **An updated PTA will be submitted prior to deploying NII-UIS in an operational environment.**

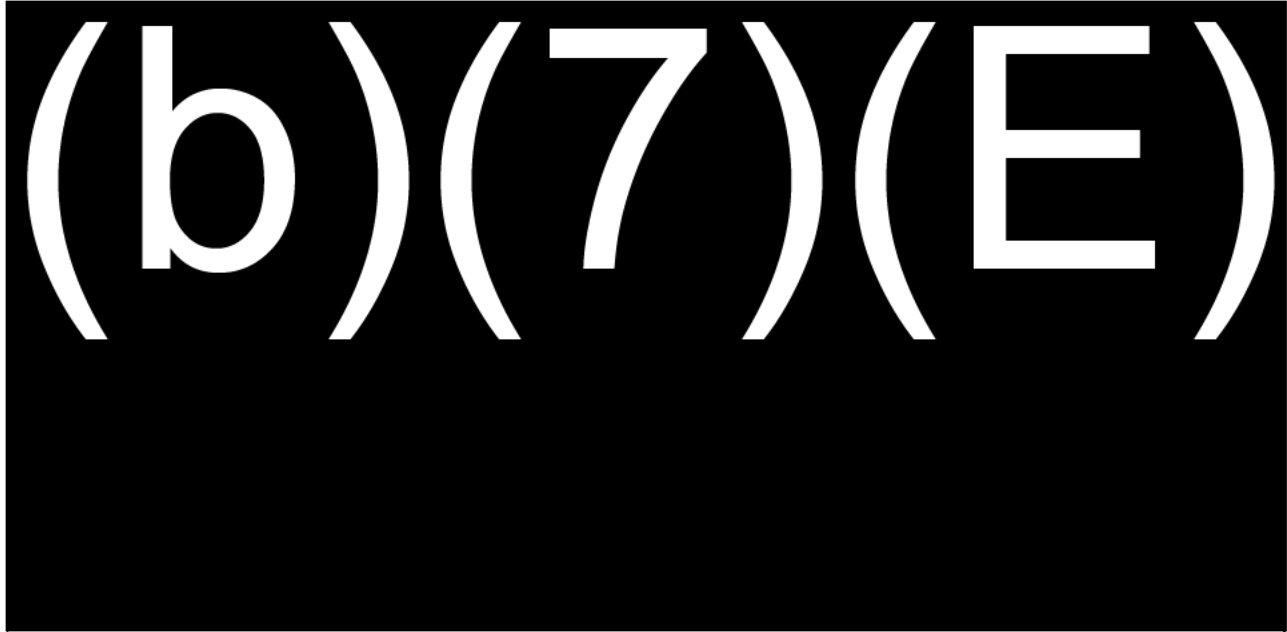
Background

The NII-UIS creates 3-dimensional images from sonar technology. (b)(7)(E)
(b)(7)(E) Reports contain plain view sight images and no PII is collected or retained on the device. Reports may be printed but again no PII is collected or retained in the report produced by the device. The NII-UIS devices do not collect any information about the encountered individual, vessel, or structure. The name of the vessel or structure's or the owner's name maybe used to label the file retained for administrative or prosecution cases. Reports generated by the NII-UIS are exclusively 3-dimensional plain view sight images.

If the UIS detects an anomaly and the encounter results in an apprehension or prosecution case, the presence of the contraband may be entered in the Tasking Operations and Management Information System (TOMIS) , e3, or Unified Secondary (USEC) and covered by that CBP system of record.

CBP will demo the NII-UIS at the Gulfport Marine unit. Training and evaluations will be conducted at several AMO marine units. CBP agents/officers receive training and must be certified in using the NII-UIS. NII-UISs will be deployed based on the operational requirements at each Branch, Sector or POE.

Figure 1 – Examples of Parasitic Devices



<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 checked="" type="checkbox"/> This project does not collect, collect, maintain, use, or disseminate any personally identifiable information²</p> <p><input type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> U.S. Persons (U.S. citizens or lawful permanent residents)</p> <p><input 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>

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.



Privacy Threshold Analysis

Version number: 06-2020

Page 5 of 11

	<input type="checkbox"/> 8 USC § 1367 protected individuals (e.g., T, U, VAWA) ³ <input type="checkbox"/> Refugees/Asylees <input type="checkbox"/> Other. Please list: <i>Click here to enter text.</i>
--	---

3. What specific information about individuals is collected, maintained, used, or disseminated?	
Reports generated by the NII-UIS are exclusively 3-dimensional images that were scanned in plain view sight. No PII is collected or retained in the NII-UIS. Results are specifically generic and printed to accompany any arrest records generated without any information that would identify the subject. If the device detects a chemical substance and the encounter results in an apprehension or prosecution case, the presence of the chemical substances may be entered in TOMIS, e3, or USEC and covered by that CBP systems of record.	
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.	
<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., <i>FIN, EID</i>) <input type="checkbox"/> Biometrics. ⁵ Please list modalities (e.g., <i>fingerprints, DNA, iris scans</i>): <i>Click here to enter text.</i> <input type="checkbox"/> Other. Please list: <i>Click here to enter text.</i>
3(b) Please provide the specific legal basis for the collection of SSN:	N/A

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)

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.



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, <i>SSN Collection and Use Reduction</i>,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?	<input type="checkbox"/> By a unique identifier. ⁷ Please list all unique identifiers used: <i>Click here to enter text.</i> <input checked="" type="checkbox"/> By a non-unique identifier or other means. Please describe: Date/Time Stamp
--	--

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. <i>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</i>	<i>Unless associated with a prosecution case, records will be retained for 30 days before being manually purged by an administrator.</i>
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)?	<i>Data is manually purged</i>

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.

⁸ See (b)(7)(E)



6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?⁹	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i>
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.	Choose an item. Please describe applicable information sharing governance in place: <i>Click here to enter text.</i>
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: <i>Click here to enter text.</i> <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 type="checkbox"/> Advanced analytics ¹⁰ <input type="checkbox"/> Live PII data for testing <input checked="" type="checkbox"/> 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)	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>

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.



(i.e., data mining)? ¹¹ This does not include subject-based searches.	
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?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>
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	<input checked="" type="checkbox"/> No. <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
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?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i>
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:

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.

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 Analysis

Version number: 06-2020

Page 9 of 11

	<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)
Date submitted to Component Privacy Office:	March 31, 2021
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	August 20, 2021
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>	
<div>(b) (5)</div>	

(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.
Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	August 20, 2021
PTA Expiration Date	August 20, 2024

DESIGNATION

Privacy Sensitive System:	No
Category of System:	Program 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



Privacy Threshold Analysis

Version number: 06-2020

Page 11 of 11

<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:	Choose an item. Click here to enter text.
SORN:	Choose an item. Click here to enter text.
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>	
<div style="background-color: black; color: white; text-align: center; font-size: 100px; font-weight: bold;">(b) (5)</div>	