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:	Automated Radiological Data Integration System - Cloud (ARDIS-C)		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	Office of Field Operations (OFO)/Non-Intrusive Inspection Division (NIID)/Systems solution Brach (SSB)/Planning, Program Analysis& Evaluation (PPAE)-Data Analysis Center-Threat Evaluation and Reduction Branch (DAC-TER)
FISMA Name (if applicable):	Automated Radiological Data Integration System Cloud (ARDIS-C)	**FISMA Number (if applicable):**	CBP-08188-MAJ-08188
Type of Project or Program:	System	**Project or program status:**	Operational
Date first developed:	January 1, 2019	**Pilot launch date:**	N/A
Date of last PTA update	July 10, 2023	**Pilot end date:**	N/A
ATO Status (if applicable):[1]	Complete	**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:	OFO/NII/SSB/PPAE Data Analysis Center – Threat Evaluation and Reduction	**Title:**	Program Manager
Phone:	(b) (6) (b) (7) (c)	**Email:**	(b) (6) (b) (7) (c)

[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)

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)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP is submitting this updated PTA to clarify the existing machine learning tools integrated within Automated Radiological Data Integration System - Cloud (ARDIS-C). These include the following:

1. Enhanced Radiological Nuclear Inspection Evaluation (ERNIE)
2. Advanced RPM Monitoring Reporter (ARMOR)
3. Advanced Analytics for X-Ray Images (AAXI)

Background

As part of the CBP mission to facilitate trade without significantly or negatively impacting the efficient movement of legitimate people and cargo across the border, the NIID DAC-TER program collects and maintains information from radiation detection and X-ray devices that inspect and screen vehicles, POV, buses, trucks, railcars, sea containers, personal luggage, and packages/parcels.

The data is collected via electronic feeds from the Radiation Portal Monitor (RPM) and Radio Isotope Identification Devices (RIID) at Port Radiation Inspection, Detection and Evaluation (PRIDE)-enabled Ports of Entry (POEs), via compact discs (CDs) from non-PRIDE-enabled POEs, and X-ray images from NII systems through the Secure Wireless Inter-Facility Transfer (SWIFT) protocol and via encrypted external hard drives.

SWIFT is an alternate way of transmitting data via wireless, leased lines, or satellite to the CBP Demilitarized Zone (DMZ) and on to ARDIS-C.

SWIFT is a data transfer mechanism only, and transfers data from RPM or NII systems to ARDIS-C. The ARDIS-C system connects to SWIFT. SWIFT will send data through ENTSD managed B2B infrastructure to a secured DMZ server. A process running on a DMZ web server will be used to transmit the data to ARDIS-C. SWIFT data are encrypted using FIPS 140-2 certified TLS 1.2 encryption. The traffic utilizes the Internet Connection Point (ICP) interface.

Information entered by the CBP officers (CBPOs) is archived for data analysis purposes (e.g., identifying companies importing shipments with higher-than-average radiation) and may include the following:

Data for operational and acquisition analysis: this includes radiological data mentioned above, along with traffic statistics (e.g., RPM use rates), maintenance work orders, PRIDE adjudication results, data about seizures from SEACATS, Optical Character Recognition (OCR) reads of container number or license plate number, deployment information, and gamma/neutron calibration information.

- Radiological data from inspections include occupancy data such as detector counts, X-ray images, duration of inspection, health and status messages from the equipment, and information about instrument configuration.
- Data for operational and acquisition analysis: this includes radiological data mentioned above, along with traffic statistics (e.g. RPM use rates), maintenance work orders, PRIDE adjudication results, data about seizures from SEACATS, Optical Character Recognition (OCR) reads of container number or license plate number, deployment information, and gamma/neutron calibration information.
- Data for pattern analysis in nuclear material trafficking: this principally comprises radiological occupancy data.
- Data for studies related to "what if" scenarios: this principally comprises radiological occupancy data as described in the previous bullet but can also include instrument configuration, equipment health and traffic statistics.
- Data for modeling and simulations of radiological threat: this principally comprises radiological occupancy data as described in the previous bullet.
- Manifest information for overland trucks, railcars, and sea containers.
- Information on medical, industrial and SNM materials that caused radiological alarms.
- Information about illicit materials via adjudication of NII systems.

A key component of the NIID DAC-TER's mission is to provide CBP sponsors and stakeholders with analysis of RPM and NII data providing intelligence and real-time insight into the CBP mission at ports POLs and POEs. These sponsors and stakeholders include: other branches within the OFO NIID, the Office of Intelligence, the LSSD, the DHS Countering Weapons of Mass Destruction Office (CWMD), the DHS Office of the Inspector General, as well as other DHS components.

ARDIS-C is the CBP system used to collect and analyze RPM and X-ray data. DAC-TER is within the NII Division and is the system owner of ARDIS-C. DAC-TER is responsible for analyzing the data for operational support and threat detection. ARDIS-C may collect PII through the PRIDE and SWIFT pipelines, CD/DVD, and the MAXIMO system. ICAM and CBP Active Directory are used for user authentication and granting access to the ARDIS-C System.

Enhanced Radiological Nuclear Inspection Evaluation (ERNIE)

1. ERNIE (Enhanced Radiological Nuclear Inspection Evaluation)

- ERNIE is a machine learning system designed to reduce false alarms and increase threat sensitivity at RPM8 sites. ERNIE also provides tools to help field officers locate sources inside inspected vehicles, so that secondary scans can be conducted more effectively. ERNIE is currently deployed in two configurations: ERNIE full (sometimes called "Standard ERNIE") which is in full operation/production at 12 seaports on 66 RPMs, and ERNIE-S (short for ERNIE-Simplified) which is in full operation/production at 13 seaports on 55 RPMs.
- Standard ERNIE includes fully integrated hardware into the remote operations flow and processes all occupancies in primary. ERNIE-S is a software only integrated solution that processes RPM8 alarms to assist in secondary inspections.

- Operations: coordinated activities to ensure effective deployment and support continued operation of ERNIE/ERNIE-S at seaports. Key components of these activities include reporting monthly performance updates, tracking the impact of hardware maintenance on ERNIE/ERNIE-S performance, defining key areas where optimization of our developed supporting technologies is necessary and coordinating with key stake holders to support field operations.
- Data Collection is conducted through the same process as all RPM data from the site supervisor computer and is radiological inspection data with additional source identification incorporated, no PII.

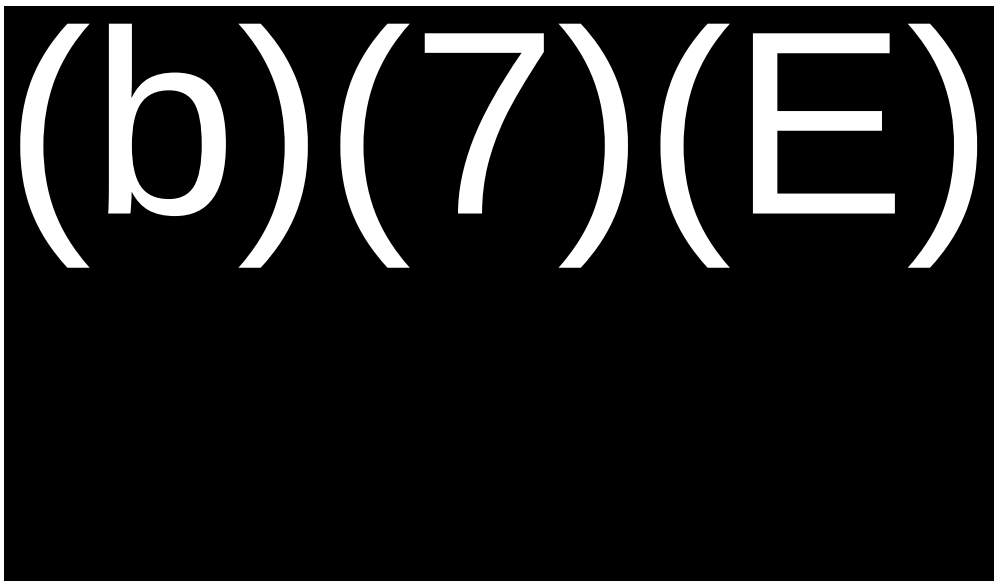


Illustration #1: ERNIE Data Flow

Vehicle Presence Sensor (VPS) Data

(b)(7)(E)

Advanced RPM Monitoring Reporter (ARMOR)

CBP is developing and is planning to fully operationalize ARMOR by the end of 2024. ARMOR is a modular software that uses machine learning to continuously assess the health of the RPM fleet, health of the individual RPMs, and the reliability of the individual parts or part types to forecast future maintenance. ARMOR predicts and address equipment failures in RPM systems before they impact operations by creating systematic monitoring and forecasting capabilities dedicated to improving awareness of the RPM fleet health. ARMOR collects RPM health data, to include:

- (b)(7)(E)

ARMOR is designed to enhance the performance of RPM systems by improving the overall health of the RPM systems.

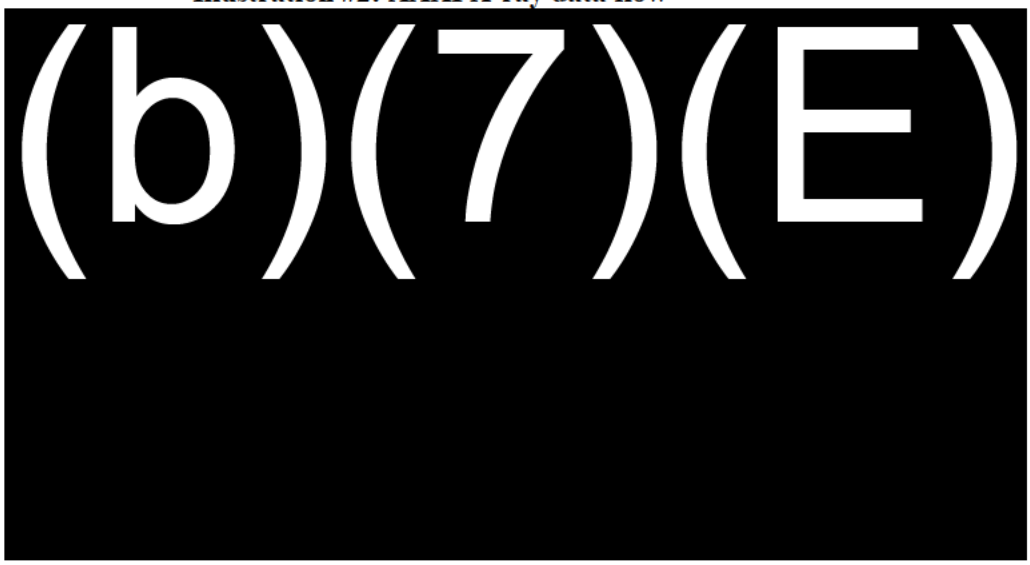
AAXI (Advanced Analytics for X-Ray Images)

- AAXI is a machine learning system designed to locate anomalies in NII (X-ray) images of vehicles crossing at a port of entry. AAXI helps adjudicate commercially owned vehicles without cargo. After verifying that there is no cargo; then isolating and categorizing each component of the vehicle, AAXI detects vehicle modifications or anomalies by alarming on large differences between the current Xray images and an expectation built from images of the same or similar

vehicles. If successful, this will vastly expedite adjudication of 30% of vehicles if applied to a single port, and much higher rates if applied across the enterprise.

- AAXI is fully cloud deployed and does not require additional hardware.
- Operations: coordinated activities to ensure effective deployment and support continued operation of AAXI at ports of entry. Key components of these activities include monitoring system for model and concept drift, defining key areas where optimization of our developed supporting technologies is necessary and coordinating with key stake holders to support field operations.
- AAXI uses the data collection already conducted through the ARDIS-C SWIFT pipeline, and includes displaying the X-Ray images, license plate information, and historical crossing instances. Additional information is not collected through AAXI.

Illustration #2: AAXI X-ray data flow



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

[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.

	☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components): Occasionally names of CBP officers assessing RDE or NII scans are captured in ARDIS-C. ☐ 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 specific description of information that is collected, generated, or retained but the CBPOs may incidentally send the information to the RDE database within ARDIS-C. This would be incidentally sent through PRIDE as it is to ARDIS today.

In the X-Ray specific section of ARDIS-C there may be PII that relates to any vehicle that has been through a scanner. This can include license plate information as well as information on the driver, shipper, consignee etc.

While there aren't specific fields containing information on individuals, the CBPOs may incidentally send the information to ARDIS-C, during adjudication and the course of secondary inspections, data captured which may contain PII such as:

- First Name
- Last Name
- Date of Birth
- Passport Numbers
- Driver's License
- Address

[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)

- City
- State
- Zip Code
- Phone Number'
- Vehicle Identification Number (VIN)
- License Plate
- In Medical Cases the Name of the Clinic treating the Individual

Additionally, there are special fields for CBPOs to enter for alarming vehicles such as:

- Consignee Name
- Consignee Address
- Consignee City
- Consignee State
- Consignee Country
- Consignee Zip Code
- Container Number
- Shipper Name
- Shipper Address
- Shipper City
- Shipper State
- Shipper Country
- Shipper Zip Code
- LPR Plate
- LPR Country
- LPR Subdivision
- LSS Contact Name
- LSS Contact Phone Number
- LSS Email Address
- Manifest Origin
- Manifest Shipper
- Truck VIN
- Truck License Plate
- Trailer License Plate
- Trailer License Issuer
- Uploaded images of vehicle may contain readable license plate and blurred image of driver taken through windshield.
- Vehicle Driver

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.

[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.

☐ 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.* ☒ 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: *Click here to enter text.* ☒ By a non-unique identifier or other means. Please describe:

[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.

[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.

	There is no ability to retrieve data by identifiers in the system and ARDIS-C does not

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]	OFO/CCS/NIID/DAC-TER is in the process of working with the CBP Records Information Management (RIM) to establish a NARA approved records retention schedule for NII data. All radiological records collected at POE (including unsolicited PII and importer PII) will be retained and disposed of in accordance with the approved NARA record retention schedule for NII data. Records will be retained in ARDIS-C until a retention schedule is approved by NARA. In the past, NARA approved indefinite retention of RDE data. The proposed retention schedule for NII data is 10 years
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)**?**	Upon approval of a retention schedule, records will be technically/automatically purged.

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: ARDIS-C receives: (a) Adjudication information for RPMs with possible PII from PRIDE; (b) X-Ray scan metadata with possible PII from MEP via SWIFT; (c) Data from MAXIMO with possible PII. ARDIS-C does not share any collected PII information with other systems.
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: *Click here to enter text.*

[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.

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: **N/A**
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: *Click here to enter text.* ☒ Yes. In what format is the accounting maintained: Any external disclosure would be documented and tracked by a completed DHS 191

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/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] 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:	0017158
Date submitted to Component Privacy Office:	May 16, 2024
Concurrence from other Component Reviewers involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	May 17, 2024

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed,

(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:	**0017158**
Date adjudicated by DHS Privacy Office:	May 20, 2024
PTA Expiration Date:	May 20, 2027

DESIGNATION

Privacy Sensitive System:	Yes
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:	**System covered by existing PIA** DHS/CBP/PIA-031 Radiation Detection 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:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

(b) (5)

(b) (5)