Privacy Impact Assessment
for the

Radiation Detection Systems

DHS/CBP/PIA-031

July 11, 2016

PRIDE Contact Point
Craig Uhl, PRIDE Project Manager
DHS/CBP/LSSD/ITB
(202) 344-1701

ARDIS Contact Point
William Fiore, ISSO
Data Analysis Center Threat Evaluation and Reduction
DHS/CBP/LSSD/ITB
(571) 468-6643

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) Radiation Detection Systems are comprised of the Port-Radiation Inspection, Detection, & Evaluation (PRIDE) System and the Automated Radiation Portal Monitor (RPM) Data Integration System (ARDIS). CBP is conducting this Privacy Impact Assessment (PIA) because both PRIDE and ARDIS collect and maintain Personally Identifiable Information (PII) in the form of importer and manifest data as well as other information taken from members of the public collected at ports of entry.

Overview

A fundamental mission of CBP is to detect and prevent terrorists and terrorist weapons from entering the United States at and between ports of entry while simultaneously facilitating legitimate trade and travel. An integral part of the CBP comprehensive strategy to combat nuclear and radiological terrorism is the scanning of all arriving conveyances and containers with radiation detection equipment prior to their release from a port of entry. PRIDE and ARDIS are designed to work in tandem to detect and report radiation threats at and between ports of entry as mandated by the Security and Accountability for Every (SAFE) Port Act of 2006.[1] PRIDE connects radiation scanning devices to the CBP network to monitor, assess, and respond to immediate radiation threats, while ARDIS automatically transmits Radiation Portal Monitor (RPM)[2] status and scanned data from the PRIDE system to the ARDIS Data Analysis Center-Threat Evaluation and Reduction Database (DAC-TER) for statistical analysis to produce intelligence and near real-time insight at all ports of entry throughout the country.

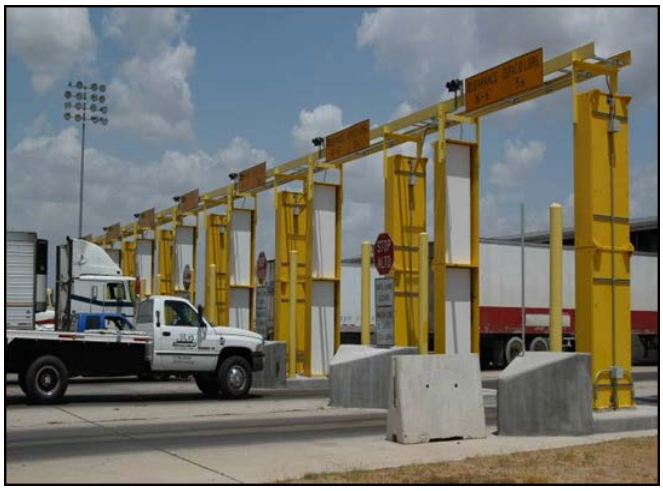


Figure 1. Radiation Portal Monitor (RPM)

[1] P.L. 109-347.

[2] An RPM is a passive detection device that provides CBP with a non-intrusive means to screen conveyances or containers (and the people operating them) for the presence of nuclear and radiological materials. RPMs passively detect energy emitted by radioactive sources that pass through it.

To accomplish this mission, the Radiation Detection Systems deploy non-intrusive equipment, such as: Radiation Portal Monitors (RPMs) (see Figures 1 and 2), Radiation Isotope Identification Devices (RIIDs) (see Figures 3 and 4, below), Visual Identification System (VIS) cameras, cargo X-ray scanners, and Optical Character Recognition (OCR) devices) at ports of entry to screen conveyances, containers, and the people transporting these conveyances or containers (commercial transport truck, privately owned vehicles, motorcycle, cargo container, bus, etc.) for the presence of weapons-grade radiological material.

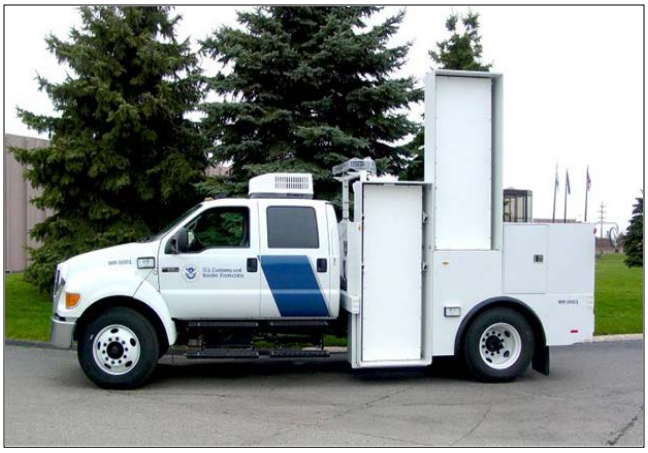
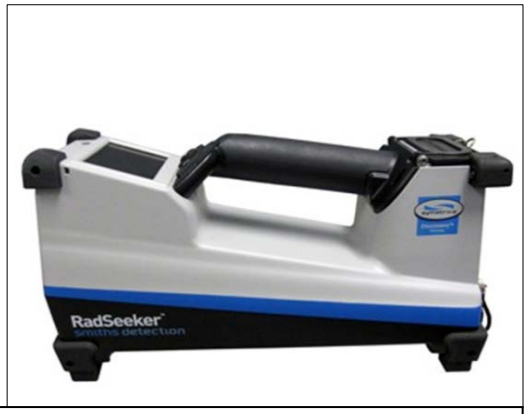


Figure 2. Mobile Radiation Portal Monitor



Figures 3 and 4: Radiation Isotope Identifier Device (RIID)

Normal Scenario

To fulfill the Department's radiation detection mission, CBP officers at all ports of entry scan all imported containers and conveyances for radiological grade material. In normal (non-alarm) scenarios, conveyances are first driven through the passive RPM (see Figure 1, above) that scans them and uploads RPM status and scan data into a local computer stationed at each port. This computer feeds into the PRIDE web service. PRIDE software transfers the data to ARDIS, which send copies of the radiation and importer data to the ARDIS DAC-TER database. PRIDE also sends filtered data (with PII removed) to a "transactional[3]" PRIDE database, which is shared

[3] PRIDE maintains data in a transactional database for 30 days to expedite data retrieval in the case of detected threats.

with DHS Domestic Nuclear Detection Office - Joint Analysis Center (DNDO-JAC) for additional analysis. Once ARDIS delivers the RPM data to the DAC-TER database, a limited subset of data is shared with the Department of Energy (DoE) Pacific Northwest National Laboratory (PNNL), which contracts with DHS to perform RPM maintenance functions.

Alert Scenario

An alert by a portal monitor indicates that the device has detected a source of radiation passing through it. An alert by itself does not necessarily mean that a nuclear weapon or harmful radiation has been detected. There are many legitimate sources of radiation, including naturally occurring radiation and various medical and industrial isotopes that pose little threat to the public. After an alarm is triggered during a primary RPM scan, CBP officers will subject the vehicle to a secondary screening either through another RPM or RIID inspection. While the primary RPM scan alerts officers to the potential presence of radiation, a secondary examination identifies the location and specific isotope triggering the alarm. Inspecting officers will attempt to positively resolve an alarm by matching the initial RPM unique numbered scan record with a more detailed unique numbered scan record from a secondary RPM through the PRIDE web service. The officer will match both scan records (by linking these records to the same conveyance) and enter the relevant determination information into PRIDE to positively adjudicate the alert and determine whether the source of radiation is a potential terrorist threat, a natural source, or a legitimate source of radiation. Depending on the determination, CBP will take the appropriate action called for in its response plans.

Pursuant to CBP policy, the CBP Laboratories and Scientific Services Directorate-Teleforensic Center (LSSD-TC) must be consulted for technical assistance whenever a radiation alert is triggered and the source of the radiation cannot be determined. Typically, inspecting CBP Officers will establish a safe perimeter and call LSSD-TC who will determine if the conveyance in question contains harmful levels of radiological material. Once LSSD-TC determines whether the radiation source is legitimate or illicit, LSSD-TC will notify the initiating officer, who will enter the information into the applicable fields in PRIDE. If the incident occurs in a PRIDE-enabled port of entry and is referred to LSSD-TC (whether the radiation is ultimately determined to be legitimate or illicit), the inspecting officer will enter the same resolution narrative into both PRIDE and TECS manually to record resolution of the radiation alarm. The resolution narrative includes: 1) the count reading from the radiation detection equipment used in the inspection, 2) isotope identification from the RIID, 3) conveyance, object, commodity, and/or shipment, and 4) a final disposition of the incident. In some cases, officers have been observed to enter unsolicited PII regarding the individuals involved in the inspection into the free text narrative field. CBP provides guidance instructing officers not to include PII when entering resolution narratives in PRIDE. This is further addressed in section 2.5.

If LSSD-TC determines that the radiation source is legitimate, once the incident report is recorded, the inspecting officer will release the shipment, conveyance, driver, and any passenger(s)

if all other entry or document requirements have been met. If LSSD-TC determines that hazardous radiological material exists or if the officers at the port of entry suspect criminal activity, LSSD-TC will provide further guidance to secure and isolate the source and notify the appropriate authorities to send radiation emergency response resources to the scene of the incident to determine the specific level of threat and response.

Overview of Port Radiation Inspection, Detection & Evaluation (PRIDE)

The PRIDE security authorization boundary is comprised of three applications which provide different user interfaces: (1) PRIDE Domestic is the radiological examination application deployed at domestic ports of entry and border crossings nationwide to scan conveyances and containers; (2) Secure Freight Initiative (SFI) supports the radiological examination of conveyances and containers at Port Qasim, Pakistan and Aqaba, Jordan, and allows U.S.-based CBP personnel to scan all containers prior to being loaded onto a ship destined for the United States; and (3) the Cargo Security Initiative-Remote Targeting (CSI-RT) web service allows CBP officers to identify high-risk conveyances and containers at foreign ports using the targeting functionality of the Automated Targeting System (ATS)[4] to make determinations on their admissibility before the containers arrive at a U.S. port of entry.

The Container Security Initiative-Remote Targeting (CSI-RT) application and the Secure Freight Initiative (SFI) application are separate and independent CBP applications grouped together with PRIDE for this PIA only.

Unless otherwise noted, throughout this PIA, "PRIDE" refers to the totality of all three of the aforementioned applications.

Port Radiation Inspection, Detection, and Evaluation (PRIDE Domestic)

PRIDE Domestic supports the Non-Intrusive Inspection (NII)[5] initiative by connecting conveyance scanning devices at domestic ports to the CBP network to allow CBP to immediately identity, assess, and respond to potential radiological threats. PRIDE is an integrated application deployed to capture and transmit real-time radiographic, spectrographic, optical, and x-ray imaging data back to centralized locations to enable efficient data sharing and analysis. PRIDE Domestic correlates that data and provides near real-time situational awareness capabilities to CBP officers for analysis and collaboration in the alarm adjudication process. PRIDE Domestic also scans the people transporting these conveyances or containers (commercial transport truck,

[4] *See* DHS/CBP-006 Automated Targeting System 77 FR 30297 (May 22, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.
[5] DHS/CBP/PIA-017 Non-Intrusive Inspection Systems Program (January 16, 2014), *available at:* http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_nii_jan2014.pdf.

privately owned vehicles, motorcycle, cargo container, bus, etc.) for the presence of weapons-grade radiological material.

Secure Freight Initiative (SFI)

The SFI application is a standalone CBP application within the PRIDE security authorization boundary. As mandated by the Security and Accountability For Every (SAFE) Port Act,[6] SFI software currently collects shipping container scan results from two ports: Qasim, Pakistan and Aqaba, Jordan. Specifically, SFI facilitates the transmission of x-ray and radiation spectrum pre-manifest data to CBP Officers in the United States. SFI software is required in order to display the information. Once the information is transmitted through the SFI port, it goes through various DHS-CBP firewalls prior to storage into the CBP's ATS-N databases to meet Office of Information Technology (OIT) security protocols. Passengers are not screened during this process.

Container Security Initiative – Remote Targeting (CSI-RT)

The CSI-RT application allows CBP officers to divert targeted high-risk ocean freight containers at foreign ports for further analysis or examination. It serves as a secure exchange mechanism to share information and exam results between CBP and host foreign governments. The CSI-RT application is an internet-based application; no software is installed on either CBP or host country computers. The CSI-RT application resides within CBP-secured internet servers. CSI-RT application security uses "https" security protocols that are hosted behind numerous CBP firewalls. All PII passes through the CSI-RT system and is stored in CBP's ATS-N databases to meet OIT security protocols. Using the CSI-RT application, a CBP officer can communicate with the appropriate foreign customs personnel and determine the need for additional information or scanning, which is ultimately uploaded into ATS. CSI-RT therefore provides the tools officers need to identify high-risk conveyances emanating from foreign ports and make determinations on their admissibility before the conveyance arrives at a U.S. port. Passengers are not screened during this process.

Automated RPM Data Integration System (ARDIS)

While PRIDE identifies immediate radiological concerns, ARDIS provides comprehensive threat analysis and a holistic overview of radiation data collected at the nation's ports of entry. ARDIS automatically transmits RPM data, such as the number of vehicles that are scanned by the RPMs and their radiation counts, from PRIDE Domestic to the ARDIS DAC-TER database for analysis. DAC-TER's mission is to provide DHS stakeholders context and interpretation from the

[6] *See* Security and Accountability For Every (SAFE) Port Act of 2006 (or SAFE Port Act), Pub.L. 109–347.

analysis of data collected by RPMs to produce intelligence and near real-time insight into the CBP mission at ports of entry.

ARDIS provides the data by an electronic connection to RPM supervisory computers via the PRIDE Domestic system to the DAC-TER database. ARDIS enables DAC-TER analysts to perform near real-time RPM data analysis on a closed CBP network. Much of the analysis done by DAC-TER analysts is in response to *ad hoc* requests from CBP Office of Field Operations (OFO) leadership and other DHS stakeholders for reports regarding radiation data. Information sent to DAC-TER for statistical analysis includes:

- Radiological data from ports of entry;
- Data for operational and acquisition analysis;
- Data for pattern analysis in nuclear material trafficking;
- Data for studies related to "what if" scenarios; and
- Data for modeling and simulations of radiological threats.

Previously, RPM records were copied from the database of the supervisory computer at the port onto compact discs. The discs were then sent via mail to DAC-TER, where the discs were uploaded to the DAC-TER database. In best case scenarios, DAC-TER analysts would receive the RPM data ten days after a vehicle or conveyance was initially scanned. However, it was common practice for ports to take months to send the RPM data to DAC-TER, presenting significant gaps in radiation threat analysis. Moreover, in transit to DAC-TER, files were frequently damaged or acquired errors requiring time consuming work by data experts to feed the DAC-TER data storage. This manual process is still used for CBP Ports of Entry (POE) not on the PRIDE system and to obtain data from the SFI and CSI-RT applications since neither system links directly to ARDIS. Information from the SFI and CSI-RT applications are sent directly to DAC-TER analysts via commercial carriers, such as USPS or FedEx.

Now, ARDIS automates the data transfers from PRIDE Domestic, expediting the process, and resulting in data availability within two to five hours after a radiological threat is detected. This allows for data to be analyzed within minutes through statistical templates or response pattern analysis in special cases for selected alarms. Once fully implemented, ARDIS will completely automate the electronic transfer of RPM, RIID, and importer information between PRIDE-enabled ports of entry and DAC-TER via the PRIDE system, supporting the Department's radiological threat analysis and prevention mission.

Free-Form Text Comment Field and Upload Capability

The PRIDE web service contains a free-form text comment field and an "Upload Files and Images" screen used by CBP officers to enter information, files, and images regarding the

conveyances and containers they inspect. These text fields may be used in cases when a vehicle sets off the alarm, and the vehicle becomes subject to additional inspection. Although PRIDE user training specifically forbids entry of PII into the system, and the system does not request or require PII to be entered, on occasion, some officers have entered PII into the comment field or uploaded documents without solicitation. As a result, PRIDE sometimes captures PII information about travelers seeking to enter the United States who are subject to port inspections. The PII entered into PRIDE has included information such as full name, social security number (SSN), passport number, alien registration number, date of birth, and driver's license number. This entry of unsolicited PII has occurred during the course of routine inspection duties and is not related to PRIDE system requirements. This PII is not used or retrieved by analysts in their evaluation of radiological data.

To help discourage the use of free-form text comment fields to convey PII, PRIDE Domestic has introduced limited-space text fields designed to support specific data entry needs when needed. The PII-fixed fields are necessary for law enforcement follow-up in the event a radioactive weapon or any suspicious circumstance surrounding the transport of radioactive material is detected. These fields give the user the ability to enter limited types of PII when the need arises. These types of fields include: vehicle license tag, vehicle state, container tag, container state, and contact information for CBP employees and contractors.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Department's legal authority to deploy radiation detection technology is authorized in the Security and Accountability for Every (SAFE) Port Act, which directs the Secretary of Homeland Security to seek and analyze data related to the shipment of cargo through the international supply chain and analyze the data to identify high-risk cargo for inspection[7], as well as to develop a strategy to screen all containers for radiation entering the United States through the highest volume ports and to deploy radiation detection equipment technology where practicable.[8] The collection of importer data by Automated Commercial Environment - International Trade Data System (ACE-ITDS)[9] (and subsequently viewed in PRIDE and ARDIS) is also authorized by the SAFE Port Act.

The collection of data involving the import and export of cargo and the entry and exit of

[7] *See* Security and Accountability for Every Port Act § 203, 6 U.S.C. § 943.
[8] *See* Security and Accountability for Every Port Act § 121, 6 U.S.C. § 921.
[9] DHS/CBP/PIA-003 Automated Commercial Environment (ACE) e-Manifest: Trucks (ACE Release 4) and International Trade Data System (ITDS) (July 14, 2006), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_aceitds.pdf

conveyances of travelers is authorized by a number of customs and immigration authorities.[10] Additionally, CBP's radiation detection program aligns with CBP's missions to enhance the efficiency of inspection and scanning systems through the use of technologies to detect and prevent the entry of hazardous materials into the United States,[11] and to expedite the processing of people and conveyances at various ports.[12]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

CBP officers at PRIDE-enabled ports of entry have access to importer data collected through ACE-ITDS. PRIDE can retrieve this information as needed using data feeds from ATS. CBP collects importer manifest data in the ACS/ACE-ITDS directly from the relevant carriers and importers and has provided notice through publications of the ACS/ACE PIA[13] and Import Information System SORN.[14]

Unsolicited PII entered into the PRIDE free-form text comment field by CBP Officers resolving radiation alarms is not retrievable using a personal identifier in either PRIDE or ARDIS, and therefore does not constitute a system of records under the Privacy Act of 1974. However, when exam information, resolution narratives, and limited-space text fields are manually entered in TECS, the radiological data and associated unsolicited PII entered into PRIDE will be covered by the TECS SORN.[15] As such, both unsolicited and importer PII may become linked with a name or other unique identifier that is retrieved within TECS. TECS provides electronic case management capability to support DHS law enforcement activities.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

PRIDE's most recent authority to operate was granted on June 24, 2013. As part of the system authorization process, a security plan for PRIDE was updated and provided for evaluation to the designated authorization authority. The information system security officer for PRIDE continues to update the security plan as needed.

---

[10] *See, e.g.*, 8 U.S.C. §§ 1221, 1357; 19 U.S.C. §§ 482, 1431, 1433, 1461, 1496, 1499, 1581-1583; and 49 U.S.C. § 44909.
[11] U.S. Customs and Border Protection Fiscal Year 2009-2014 Strategic Plan, Goal 1.2, available at: http://www.cbp.gov/sites/default/files/documents/strategic_plan_09_14_2.pdf.
[12] U.S. Customs and Border Protection Fiscal Year 2009-2014 Strategic Plan, Goal 2.1, available at: http://www.cbp.gov/sites/default/files/documents/strategic_plan_09_14_2.pdf.
[13] DHS/CBP/PIA-003(b) Automated Commercial Environment (ACE) (July 31, 2015), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-cbp-ace-july2015.pdf.
[14] DHS/CBP/-002 Import Information System 80 FR 49256 (Aug. 17, 2015) *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-08-17/html/2015-19731.htm.
[15] DHS/CBP-011 U.S. Customs and Border Protection TECS 73 FR 77778 (Dec. 19, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

ARDIS is a new radiation data analysis system. An interim authority to operate was granted by the CBP Office of Information and Technology (OIT) on June, 24, 2013. The authority to operate became effective June 26, 2014. A security plan has been developed for ARDIS.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. CBP is in the process of determining a retention schedule with NARA. All radiation records collected at ports of entry and entered into PRIDE (including unsolicited PII and importer PII) will be retained and disposed of in accordance with a records schedule approved by NARA. Records will be retained in the ARDIS DAC-TER database on a permanent basis until a retention determination is made by NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Neither PRIDE nor ARDIS are subject to the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

PRIDE collects information recorded by radiation detection equipment at domestic and international ports, as well as three types of PII: 1) importer data that is extracted from the Automated Commercial System (ACS) and the Automated Commercial Environment-International Trade Data System (ACE-ITDS) or auto-populated into the PRIDE web service by an ATS data feed.2) supplemental information captured using designated limited-space text fields used on an as-needed basis; and 3) unsolicited PII that is sometimes entered into the PRIDE web service by CBP officers when resolving radiation alarms at ports of entry. Both types of PII are transmitted to ARDIS through the PRIDE network and are viewable by PRIDE and DAC-TER data analysts, in their respective databases.

ARDIS sends RPM activity data from the PRIDE system web service to its DAC-TER database for statistical analysis. Through an automated process, ARDIS DAC-TER extracts importer and manifest information from PRIDE into the DAC-TER database also for data analysis purposes. At ports of entry, CBP officers resolving radiation alarms will enter the container number, bill number, and shipping code into PRIDE to initiate data feeds from ACS/ACE-ITDS

via ATS as needed, the data feeds will auto populate the remaining cargo fields into the PRIDE web service.

Importer PII includes:

1. Cargo Manifest Information (including quantity and description)
2. Carrier Name
3. Consignee Name
4. Consignee Address
5. Consignee City
6. Consignee State
7. Consignee Zip Code
8. Carrier Name
9. Shipper Name
10. Shipper Address
11. Shipper City
12. Shipper State
13. Shipper Zip Code
14. Container Number

Other information contained within PRIDE includes:

1. Vehicle License Plate Number (Tag);
2. Vehicle State;
3. Container Tag;
4. Container State;
5. LSS[16] Contact Name;
6. LSS Contact Phone;
7. LSS Contact Fax;
8. Officer Hash ID;

[16] Laboratories and Scientific Services.

9. Officer Name;
10. Officer Phone.

The PRIDE system was not designed initially to collect PII aside from the listed importer PII. However, some CBP officers, on occasion have entered PII into the comments field on the PRIDE web service when resolving radiation alarms. Though officers entering PII is rare, information including but not limited to full names, dates of birth, alien registration numbers, and driver's license numbers have been entered into PRIDE. To address this issue, short designated text fields were introduced to enable users to add relevant PII on an as-needed basis. The type of PII added in these fields are labeled to prevent the addition of PII that is not relevant nor needed, such as SSNs. This PII is then passed to ARDIS via the PRIDE network. Unsolicited entry of PII into the free-form text comment field by CBP Officers into the PRIDE system is neither searchable by, nor useful to either PRIDE or DAC-TER data analysts and is not relevant to CBP's radiation detection and analysis missions.

2.2 What are the sources of the information and how is the information collected for the project?

PRIDE collects information from three sources: 1) Information recorded by radiation detection equipment at domestic and international ports. 2) Importer PII and manifest information extracted from ACS/ACE-ITDS; and 3) In some cases, information collected from members of the public and entered by the CBP Officer at the port of entry in either designated limited-space text fields, the free-form text comment field, or uploaded images. These text fields may be used in cases when a vehicle sets off the alarm, and the vehicle becomes subject to additional inspection. Officers can collect PII from people seeking entry to the U.S. at the port of entry, or based upon the officer's observation. All collected data is then transmitted via a secure network to the PRIDE database or to the DAC-TER database through the ARDIS application.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Neither PRIDE nor ARDIS use information from commercial data sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The PRIDE and DAC-TER databases rely on internal software controls and communication protocols to ensure the accuracy and integrity of the data from the port supervisory computer to the PRIDE web service. Both PRIDE and ARDIS form a near real-time radiation

detection and analysis system. Radiation detection events cannot be replicated or repeated to ensure accurate reporting.

The accuracy of any unsolicited PII entered by a CBP Officer during an inspection is dependent on the officer's review of official documents such as driver's licenses, passports, titles, bills of lading, and other documents. The accuracy of such information is contingent upon the officer's manual input of information into PRIDE and the authenticity of the documents inspected by the officer.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: CBP Officers may enter irrelevant or unnecessary PII into the free-text fields to accomplish the purposes of CBP's radiation detection program.

Mitigation: To mitigate the collection of irrelevant or unnecessary PII, CBP implemented several updates for the PRIDE system. First, the free-form text field displays a banner, which says, "Do Not Enter PII into Comments Box.' The word "PII" contains a hyperlink, which will lead to an internal CBP webpage that defines PII and refers users to the CBP Privacy Office for further information, if needed. The "Upload Files and Images" screen also bears a similar banner and links to a definition of PII. Additionally, limited-space data fields have been added to reduce the need to add data into the free-form field. These limited data fields are labeled to receive specific information as listed earlier in this Section. Also, the internal Standard Operating Procedures (SOP) is in the process of being revised to prohibit PII in PRIDE and will warn that inclusion of PII will trigger a privacy incident, reportable to the CBP Privacy Office. Finally, notifications were developed and distributed to the field as reminders to officers not to enter PII into PRIDE.

Privacy Risk: PRIDE collects importer PII, manifest information, and other PII that exceeds the minimal amount of data necessary for CBP to fulfill its radiation detection mission.

Mitigation: PRIDE collects importer and manifest data to support the CBP mission to resolve all radiation detection alerts at POEs. The front-line officer needs to determine whether an identified radiation source is legitimate or a threat. To response quickly to mitigate alarms, the officer must know the shipment ID, commodity, shipper, and/or consignee, etc. to make an accurate determination. The collected importer and manifest data provides the officer with the information needed to make this real-time assessment.

For example, shipments containing porcelain or steel may contain a specific level of radiation that is normal for that commodity and quantity. The officer is able to use the importer and manifest data to make an informed decision to adjudicate the possible threat. The data is also collected to develop algorithms to determine the risk for similar future shipments. In addition, this information provides support to investigative/law enforcement inquiries, in the event that an incident occurs after entry.

The PII-fixed fields are necessary to resolve potential or realized radiation risk. The fields collect information regarding: vehicle license tag, vehicle state, container tag, container state, and contact information for CBP employees and contractors. In addition, this information is used for law enforcement follow-up in the event a radioactive weapon or any suspicious circumstance surrounding the transport of radioactive material is detected.

Privacy Risk: Some information in PRIDE is manually entered by CBP Officers, based on the official documentation provided. There is a risk that CBP Officers may inadvertently enter inaccurate information manually into PRIDE.

Mitigation: This risk is partially mitigated by the infrequency in which data is manually input into PRIDE. Not all data in PRIDE is manually entered by CBP Officers. Importer information is entered into PRIDE via a system to system transfer, thus enhancing the accuracy of the data. However, inaccuracies are always a risk in situations when individuals manually enter data into a system. On occasion, CBP Officers manually input data when an alert signals a potential threat, and additional information is needed to identify and resolve the threat.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Importer Information

Importer information, which may contain PII related to the consignee, shipper, shipping company, and cargo contents, is used to investigate and resolve radiation alarms. The importer information is extracted from the Automated Commercial System (ACS) and the Automated Commercial Environment - International Trade Data System (ACE-ITDS), which CBP uses to track, control, and process all commercial goods imported into the United States. Importer information is also auto populated into fields in the PRIDE web service via the Automated Targeting System (ATS). Importers submit the required manifest data elements into ACS/ACE-ITDS and the data is immediately sent to the CERTS module[17] of ATS to support targeting purposes, and then returned to ACS/ACE-ITDS for retention. CBP officers resolving radiation alarms at PRIDE-enabled ports of entry will enter the container number, bill number, and shipping code into the PRIDE web service, and retrieve data feeds from ATS. These data feeds will auto populate the remaining importer and cargo fields.

[17] Cargo Enforcement Reporting and Tracking System (CERTS) provides CBP officers with a user-friendly, single point of entry for exam findings data. It also allows the CBP officer to query and build custom reports. CERTS establishes a historical database linking targeting reasons, risks, issues, actions, decisions, events, and past and present findings with commodities, shipping parties, and manifest information. CERTS allows trend analysis on the targeting rules based on historical enforcement information. For a detailed description of the ATS cargo targeting rules, *see* DHS/CBP/PIA-006(b) Automated Targeting System (June 1, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats006b_0.pdf.

PRIDE delivers importer information to the ARDIS DAC-TER database for analysis via an automatic data feed. Importer PII and manifest data allows DAC-TER analysts to conduct advanced radiation analysis, including determining which companies are importing shipments with higher than average radiation counts, or to generate radiation intelligence reports based on shipments imported from specific countries of origin. Moreover, importer PII has a potential law enforcement purpose that could facilitate investigations should illicit levels or types of radiation be identified when the conveyances are scanned at a port.

Importer data is useful to DAC-TER analysts for advanced radiation analysis including determining which companies are importing shipments with higher than average radiation counts, or generating radiation intelligence reports based on shipments imported from specific countries of origin. DAC-TER shares RPM data with PNNL, a DHS DNDO contractor, which provides a number of RPM maintenance-related services to CBP OFO including: RPM installation, RPM maintenance, software upgrades, and RPM calibration. All PII and cargo manifest information is removed before the record is transmitted to PNNL. To date, records have not been shared with any other entities outside of CBP.

All ACS/ACE-ITDS and ATS privacy compliance requirements are outlined in the ACS/ACE-ITDS PIA and Importer Information System of Records Notice (SORN) and the ATS PIA and SORN respectively.

Radiation Detection Information

PRIDE facilitates the scanning, review, and adjudication of containers, vehicles, and other items of interest at domestic and selected foreign ports for the presence of illicit nuclear material that could threaten national security. PRIDE reports information related to radiological alarms to analysts who can determine whether there is a security threat.

ARDIS provides radiation data collected at ports of entry to the DAC-TER database via the PRIDE network. DAC-TER's mission is to provide CBP and other DHS stakeholders context and interpretation from the analysis of radiation data collected from scanned conveyances at ports of entry to produce intelligence and near real-time insight into the CBP mission at ports throughout the country.

The radiation information collected at ports of entry is necessary to resolve radiation alerts and to provide analysts with near real-time situational awareness of port security throughout the country. Importer PII and manifest data is useful to ARDIS DAC-TER analysts for advanced radiation analysis including determining which companies are importing shipments with higher than average radiation counts, or generating radiation intelligence reports based on shipments imported from specific countries of origin. Moreover, importer PII and other PII collected has a potential law enforcement purpose and could facilitate investigations should illicit levels or types of radiation be identified when conveyances are scanned at the port.

Manual Entry into TECS

In the event that the RPM generates an alarm for the item being scanned, officers place the item on "hold" for possible secondary scanning, and they contact LSS for further consultation. It is specifically in these types of situations that they use TECS to manually record that the item in question was placed on hold. As stated earlier, this is a manual entry of information into TECS. PRIDE, in turn, contains a field in which the associated TECS number for the item is entered manually by the officer.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. CBP Officers use ATS-N manifest data, which provides an assessment of risk criteria, to determine which shipments warrant further attention.[18] Using the CSI-RT application, CBP Officers can communicate with the appropriate foreign customs personnel and determine the need for additional information or scanning, which is ultimately uploaded into ATS. Often this additional screening will satisfy the officer's concerns and the case can be resolved. Physical inspections of the conveyance in question may also be requested by officers if the requests for additional information or scanning prove unsatisfactory. CSI-RT therefore provides officers with a mechanism to request further inspection of high-risk shipments emanating from foreign ports and make determinations on their admissibility before the conveyance arrives at a U.S. port.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. However, under normal radiation detection scenarios, PRIDE shares some radiation data collected at ports of entry with the DHS DNDO Joint Analysis Center Collaborative Information System (JACCIS) via an encrypted network soon after it is recorded in the PRIDE transactional database. The data shared includes alarm notifications, alarm status, reach back query, and general computational services. Radiation data collected by PRIDE is shared with the JAC to facilitate DNDO's strategic objective of developing the global nuclear detection and reporting architecture. The PRIDE data delivered to DNDO allows the JAC to correlate alarms worldwide to identify any potential radiological threats. DNDO JAC only receives a limited subset of PRIDE data to accomplish their strategic objectives and all PII is removed from the PRIDE record before transmission to the JACCIS.

[18] For a detailed description of the ATS cargo targeting rules, *see* DHS/CBP/PIA-006(b) Automated Targeting System (June 1, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats006b_0.pdf.

A limited subset of non-PII data is also shared with Pacific Northwest National Laboratory (PNNL), which contracts with DHS to perform RPM maintenance functions.

Under an alert scenario, CBP Officers must consult with the CBP Laboratories and Scientific Services Directorate-Teleforensic Center (LSSD-TC) for technical assistance whenever a radiation alert is triggered and the source of the radiation cannot be determined. If the incident occurs in a PRIDE-enabled port of entry and is referred to LSSD-TC (whether the radiation is ultimately determined to be legitimate or illicit), the inspecting officer will enter the same resolution narrative into both PRIDE and TECS manually to record resolution of the radiation alarm. The resolution narrative includes: 1) the count reading from the radiation detection equipment used in the inspection; 2) isotope identification from the RIID; 3) conveyance, object, commodity and/or shipment; and 4) a final disposition of the incident. In some cases, officers have been observed to enter unsolicited PII regarding the individuals involved in the inspection into the free-text narrative field. CBP provides guidance instructing officers not to include PII when entering resolution narratives in PRIDE.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the CBP Officers may forward information from the free-text narratives to the LSSD-TC, DNDO, or PNNL, despite no nexus to a radiation threat.

Mitigation: This risk is mitigated because CBP Officers only forward the unsolicited data stored in the free text fields to the LSSD-TC, to support their findings to the LSS, and so that the LSS can provide recommendations to the CBP Officer to assist the Officer in making a decision to release or not release the cargo or person. The PII-fixed fields are necessary for law enforcement follow-up in the event a radioactive weapon or any suspicious circumstance surrounding the transport of radioactive material is detected. CBP Officers do not forward information in the free-text fields to DNDO or PNNL.

Privacy Risk: There is the potential risk of unauthorized access, use, or disclosure of radiation data from PRIDE or ARDIS.

Mitigation: All PRIDE and ARDIS data is protected by the technical, operational, and management security controls identified and defined by NIST[19] and DHS 4300A directives. Compliance with these controls is monitored and enforced by a full-time information system security officer and governed by DHS and CBP guidance. All PRIDE and ARDIS security controls are tracked and monitored in official Security Plans by the ISSOs.

Both PRIDE and the DAC-TER databases employ user controls that limit the access and functions that individual users may perform within either PRIDE or ARDIS. Furthermore, all persons working in DAC-TER must pass a full background investigation from CBP and be granted

[19] *See* Nat'l Inst. of Standards and Tech., Recommended Security Controls for Federal Information Systems and Organizations (2009).

a Hash ID. All such persons must also sign a nondisclosure agreement and must pass the "CBP IT Security Awareness and Rules of Behavior" training prior to being granted access to the database.

The process for granting user access to PRIDE is summarized as follows. When a potential user completes the application for a PRIDE account, then his/her supervisor identifies what PRIDE system role is needed to complete their job. The System Owner determines the conditions for role membership. These conditions are enforced by account managers at the first stage of review, when they review submissions of prospective users. The System Owner has designated the account managers as the approvers for requests to create information system accounts. All accounts for PRIDE are reviewed annually by the user's supervisor to confirm whether there is still a need-to-know based on his or her role. If modifications to the users account are needed, the supervisor will notify OFO and OFO will in turn notify CBP OIT (Office of Information Technology). All PRIDE user roles are described in the PRIDE Security Plan (SP), which is maintained by the ISSO.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Importers provide their own shipping and manifest information to CBP through ACS/ACE-ITDS every time they have a shipment. During the creation of an ACE user account, importers are provided a Privacy Act Statement regarding the authority of CBP to collect the requested information and how the Agency uses the information. In addition, signs are posted at all PRIDE Domestic sites as notice for people transporting conveyances or containers that they are passing through a radiation portal monitor. CBP also provides notice through the ACE PIA and the Import Information System (IIS) regarding the collection and use of PII by ACS/ACE-ITDS, as well as through the publication of the laws and regulations authorizing the collection of such information.

Radiological incidents that require consultation with LSSD-TC are documented in resolution narratives that are entered into TECS, in some cases along with the aforementioned unsolicited PII. As a result, opportunities for individuals to consent to particular uses of this information are addressed in the TECS SORN. Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, TECS is exempt from Section (e)(3), which requires notice be given to individuals from whom information is collected. Therefore, there is effectively no consent mechanism other than the choice of whether to travel or ship merchandise.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The decision to import goods and merchandise into the United States is within the discretion of the individual. U.S. law requires importers to provide certain information to allow CBP to determine whether the goods and merchandise may enter the United States, and are in compliance with relevant export requirements. Information (including importer PII) is collected by ACS/ACE-ITDS and retrieved by PRIDE through a data feed with ATS. This importer information is mandated by U.S. law. Therefore, declining to provide importer PII would prohibit an individual from shipping any goods or merchandise to the United States.

The collection of PII by CBP Officers, when it occurs, happens during the course of their routine inspection duties and is not related to PRIDE system requirements. As noted previously in this PIA, importer and manifest information is collected in ACS/ACE-ITDS and auto-populated in PRIDE via a data feed with ATS. Similarly, all radiological incidents that require consultation with LSSD-TC are documented in resolution narratives that are entered into TECS. Opportunities for individuals to consent to particular uses of this information are addressed using the processes defined by these systems. As most information collected by these systems is mandated by law, there is effectively no consent mechanism other than the choice of whether to travel or ship merchandise.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is the potential risk of collecting PII of inspected individuals without providing notice or without the consent of the individual.

Mitigation: This risk is partially mitigated through the posting of signs at all PRIDE Domestic sites as notice for people transporting conveyances or containers that they are passing through a radiation portal monitor. Items that trigger alerts are subject to additional inspection resulting in the collection of additional information. Since people are present during these inspections, they are aware of the additional PII collected about them by CBP at these PRIDE-enabled ports of entry.

In addition, the public is provided general notice of PII collection through the publication of this PIA. No additional notice is given because PRIDE does not require or solicit individual PII.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

CBP is working with the CBP Records Management Office to finalize the proposed 25-year retention schedule for DAC-TER. DAC-TER database records are currently retained on a

permanent basis until a final retention determination is published by NARA. Records are retained in the DAC-TER database to fulfill reporting and RPM maintenance functions. For example, OFO and the Office of Intelligence (OI) require reports that combine regulatory and trade information dating back to the inception of the RPM program. DAC-TER analysts require the full RPM life cycle of data for use in calibrations, RPM aging analysis, and the development of statistical tools. Currently, ARDIS stores RPM records since the inception of the RPM program in 2003. The DAC-TER database also contains radiation data from non-PRIDE enabled ports of entry.

The PRIDE program is working with CBP Records Management to finalize a record retention schedule for the transactional database. Once the data is collected by the PRIDE web service, the data is quickly transferred to a holding PRIDE transactional database. Records in the transactional database are only viewable for 30 days, at which point the records are moved to DAC-TER. The transactional database holds the records for 30 days to improve accessibility by the PRIDE application and allow a quick turnaround time for the retrieval and uploading of secondary files. Without the transactional database, the efficiency of PRIDE would be compromised due to the large volume of data the system would have to sift through.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that RPM data, CBP Officer-collected PII, and importer PII collected at ports of entry may be retained for a longer period than necessary for the purpose for which the data was collected.

Mitigation: This risk is only partially mitigated. A NARA retention schedule has not yet been published for data collected by PRIDE and ARDIS. Once published, records will be securely retained and disposed of in accordance with the retention schedule, thereby minimizing the risk of excessive records retention. For PRIDE, the proposed record retention schedule is a 30-day retention period for its transactional PRIDE database. ARDIS is working within CBP to establish an appropriate record retention schedule for its DAC-TER database. Until the ARDIS record retention schedule is established, the data is designated as permanent.

Importer PII and cargo data is useful to PRIDE users to identify potential high risk conveyances and for advanced radiation analysis or to facilitate a law enforcement investigation in the event that an illicit level or type of radiation is identified. To guard against excessive retention, all data is migrated from the PRIDE transactional database to the DAC-TER database after the 30-day period. Once the data transfer is complete and a NARA retention schedule is published, any new importer PII and cargo data ingested from ACS/ACE-ITDS through the ATS feed will be retained in the DAC-TER database in accordance with the record retention requirements of those systems, or the retention period for ARDIS, whichever is shortest. PII collected by CBP Officers at the port of entry will also be subject to the established retention schedule once approved by NARA.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Data collected by PRIDE or ARDIS is not shared outside of DHS as part of normal agency operations. If there would be any instances where data would be shared outside CBP on a regular basis, then a Memorandum of Understanding (MOU) would be drafted and reviewed by the program manager, component privacy officer, Office of Chief Counsel, and then sent to DHS for formal review.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Data collected by PRIDE or ARDIS is not shared outside of DHS as part of normal agency operations. However, in the event that an illicit level or type of radiation is identified and other law enforcement agencies must be contacted, any information collected by PRIDE could be provided to law enforcement agencies to facilitate their investigation. The TECS and ACS/ACE-ITDS SORNs set forth routine uses that permit the sharing of case information, such as with law enforcement and prosecutorial entities or as part of litigation as described. This sharing is compatible with CBP's law enforcement and border security missions.

6.3 Does the project place limitations on re-dissemination?

Not applicable. RPM data collected by PRIDE or ARDIS is not shared outside of DHS as part of normal agency operations. However, if a case did arise in which information was shared outside the Department, limitations on re-dissemination would be outlined as part of a MOU.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

DAC-TER maintains a database of all data and reports it produces. While radiation data is not shared outside of DHS as part of normal agency operations, *ad hoc* requests for reports may be made in the future by Government entities outside the Department. Any information shared outside DHS on a regular basis will be tracked using a MOU and would be reviewed by the program manager, CBP Privacy Officer, Office of Chief Counsel, and then sent to DHS for formal review.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no risk to information sharing because PII is not shared outside of DHS from PRIDE or ARDIS. However, in the event that an illicit level or type of radiation is identified and

other law enforcement agencies must be contacted, any information collected by PRIDE could be provided to law enforcement agencies to facilitate their investigation. The TECS and ACS/ACE-ITDS SORNs set forth routine uses that permit the sharing of case information, such as with law enforcement and prosecutorial entities or as part of litigation as described. This sharing is compatible with CBP's law enforcement and border security missions.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of, and access to, any record contained in PRIDE or ARDIS or seeking to contest its content, may gain access to certain information about them by filing a Freedom of Information Act (FOIA) or Privacy Act request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection
FOIA Division
90 K Street, NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

More information is available at: http://www.cbp.gov/xp/cgov/admin/fl/foia/.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

All PII is provided by the requestor at time of inspection at the port of entry, and not by a third party. Therefore, the onus is on the individual to provide accurate information about him or herself to CBP officers during the course of radiological inspections. Since PRIDE prohibits users from entering PII into the system, official procedures are not in place to correct erroneous entry.

If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

Customer Service Center
OPA MS: 1345
U.S. Customs and Border Protection
1300 Pennsylvania Avenue, NW
Washington, DC 20229

7.3 How does the project notify individuals about the procedures for correcting their information?

Through the publication of this PIA, individuals seeking notification of and access to any record contained in either PRIDE or ARDIS are informed that they may submit a request through the procedures in 7.1 and 7.2, above. In addition, CBP has an Executive Communications Branch in its Office of Field Operations to provide redress with respect to incorrect or inaccurate information collected or maintained by its electronic systems (including ACS/ACE-ITDS). If an individual believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to the Customer Service Center, at the following address:

Customer Service Center,
OPA - MS-1345
U.S. Customs and Border Protection,
1300 Pennsylvania Avenue, NW
Washington, DC 20229.

Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue. Individuals may provide additional information to CBP to ensure that the information maintained by CBP is accurate and complete. The Customer Service Center will respond in writing to each inquiry.

ACS/ACE-ITDS is the source system for importer PII in PRIDE. Accordingly, any individual seeking corrections of importer information collected by ACS/ACE-ITDS should contact the CBP Customer Service Center and follow the redress procedures outlined above.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know that their information is in PRIDE and ARDIS and therefore be unable to correct inaccurate information through the redress process.

Mitigation: This risk is partially mitigated. Importers have the ability to access and correct their own information through ACE, the source system that provides importer information to PRIDE. Since importers provide their own information during the application process and prior to every shipment, that information should be timely and accurate. Individuals that file electronically may view and correct their information prior to submission and before ACE accepts the transmission. To gain access to non-public information importer information, the individual may request information about his or her records through the FOIA process described in this section.

Signs are posted at every PRIDE Domestic site providing notice for people transporting conveyances or containers that they are passing through a radiation portal monitor. Items that trigger alerts are subject to additional inspection resulting in the collection of additional information. Since people are present during these inspections, they are aware of the additional PII

collected about them by CBP at these PRIDE-enabled ports of entry. This PIA provides information describing how to obtain and correct information collected at these ports and maintained in PRIDE and ARDIS.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The controls in place to ensure that information is handled in accordance with the above described uses include:

User Roles – In both PRIDE and ARDIS, the use and access to information is based on the role assigned to a particular user. All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and responsibilities of each user. Access by users, managers, system administrators, developers, and others to the PRIDE and ARDIS data is defined in the same manner and employs controls to tailor access to mission or operational functions. PRIDE and ARDIS user roles are highly restricted and audited. Access is restricted in the form of role-based access, which is determined through a demonstrated need to know and the requirements of a particular job function.

The data collected by PRIDE and ARDIS may only be accessed using the secure CBP network with encrypted passwords and user Hash ID sign-on functionality. All PRIDE and ARDIS users are required to complete security and data privacy training on an annual basis and their usage of the systems is audited to ensure compliance with all privacy and data security requirements.

Audits – Every three years, the PRIDE system undergoes an internal system test and evaluation process conducted by CBP OIT. This process includes interviews with the information system security officer, program manager, and development and maintenance teams to verify that NIST security controls are being followed correctly. The process also includes in-depth system scans to identify technical control weaknesses that are then corrected by the information system security officer. Furthermore, the PRIDE program conducts an annual self-audit culminating in a self-assessment requiring the PRIDE Information System Security Officer (ISSO) to re-assess at least one third of the relevant NIST Special Publication 800-53 security controls.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All PRIDE and ARDIS users are required to complete annual training in the CBP Virtual Learning Center training courses on privacy including: "Protecting Personal Information" and "CBP IT Security Awareness and Rules of Behavior Training." Each of the Virtual Learning Center security trainings cover what constitutes PII and how to handle PII. If an individual does

not complete the training, access to PRIDE or ARDIS will be lost. User access is integral to the performance of assigned duties, therefore failing to complete the required privacy trainings could jeopardize the individual's continued employment with CBP.

Additionally, all potential PRIDE users must take PRIDE user training before being granted access to the system. PRIDE user training specifically forbids entry of PII into the PRIDE free-form Text comment field.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

PRIDE user access is restricted based on the user's role. User access is enforced by the user's role-based access, and roles are assigned only after supervisor request and appropriate security checks have been confirmed. PRIDE user roles are grouped into administrative, supervisory, officer, and threat response roles. Some functions are enabled across more than one role.

PRIDE users must have current background investigations. PRIDE users receive the lowest level privilege necessary to perform their specific job. Access to PRIDE functionality is extremely restricted and requires approval of a user's supervisor based on the particular role that is required to perform the job function. Initial requests are made when both the supervisor and CBP user complete an access request form. This form is forwarded by the supervisor via email to a security group, who verifies that a background investigation has been successfully adjudicated. The request is then sent from the supervisor to either CBP OFO or CBP Office of Intelligence (OI) for further examination to ensure that the user is granted the appropriate credentials. Once complete, OFO or OI sends an encrypted request to the ATS hotline advising them of what roles or privileges a user is to be granted.

All accounts for PRIDE are reviewed annually by the users' supervisor at the request of OFO to ensure that there is still a need to know based on his or her role. If modifications to the user's account are needed, the supervisor will notify either OFO or OI who will in turn notify ATS security indicating that a user's access needs to be modified (*i.e.*, deactivating, upgrading, or downgrading PRIDE access privileges).

ARDIS employs user controls based on read-only accessibility. Certain ARDIS user administrators may make certain changes to the information for data quality issues (e.g., if a date was entered in the future). While any ARDIS user can perform searches of RPM data collected at the ports of entry, importer PII and manifest information can only be searched by a limited number of users who are responsible for developing *ad hoc* reports on radiation data. DAC-TER access is granted by the DAC-TER government lead or project manager. Access is granted, by Hash ID, on

a limited basis based on job requirements. Persons who do not have a need to know of certain restricted data elements are not granted access to them.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

PRIDE and ARDIS DAC-TER information is not shared outside of DHS, unless it is shared from TECS as law enforcement information. Any information sharing agreement or MOU related to information sharing of either PRIDE or DAC-TER data outside of DHS would be reviewed by the program manager, Component Privacy Officer, and counsel and then sent to DHS for formal review. In addition, any new uses of the system's information or new access to the system by organizations within or outside DHS, would require preliminary review by the program and Component Privacy Officer to determine the extent to which further review and evaluation is needed.

Responsible Officials

Craig Uhl
PRIDE Project Manager
DHS/CBP/LSSD/ITB

William Fiore, ISSO
Data Analysis Center Threat Evaluation and Reduction
DHS/CBP/LSSD/ITB

Debra L. Danisek
CBP Privacy Officer (Acting)
U. S. Customs and Border Protection

Approval Signature

Original signed copy on file with DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security