Privacy Impact Assessment
for the

Non-Intrusive Inspection Systems Program

DHS/CBP/PIA-017

January 16, 2014

Contact Point
William Romero
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1376

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

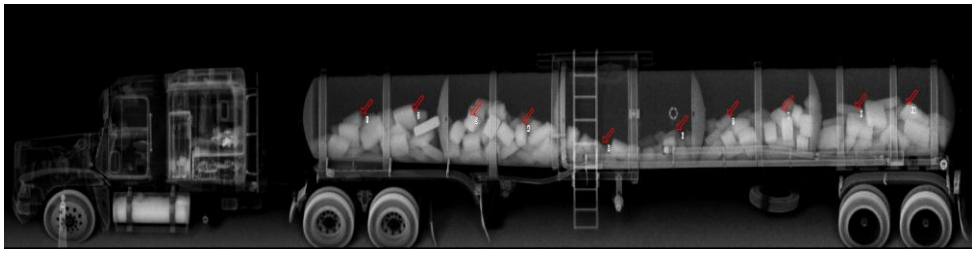
Abstract

Part of the Department of Homeland Security (DHS), U.S. Customs and Border Protection's (CBP) mission is to facilitate legitimate international trade. The Non-Intrusive Inspection (NII) Systems Program furthers this mission by providing technologies to inspect and screen conveyances or cars, trucks, railcars, sea containers, as well as personal luggage, packages, parcels, and flat mail through either x-ray or gamma-ray imaging systems. CBP Officers use NII systems to help them effectively and efficiently detect and prevent contraband, including drugs, unreported currency, guns, ammunition, and other illegal merchandise, as well as inadmissible persons, from being smuggled into the United States, while having a minimal impact on the flow of legitimate travel and commerce. The imaging system used on the conveyance itself collects photographic and other images that may contain personally identifiable information (PII), such as vehicle identifiers (e.g., license plate numbers). CBP is conducting this Privacy Impact Assessment (PIA) pursuant to Section 208 of the E-Government Act of 2002[1], because NII systems use information technology to collect, maintain, and disseminate PII in the form of scanned, photographic, or video images. However, NII cannot retrieve the PII by personal identifier (e.g., name); therefore use of NII does not require CBP to conduct a system of records notice pursuant to the Privacy Act of 1974.[2]

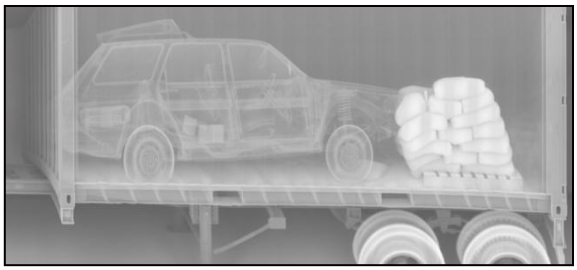
Overview

NII Technologies

To "see" into conveyances and identify potential contraband, the NII Systems Program deploys two types of NII imaging systems – Large-Scale and Small-Scale. Large-scale NII imaging systems are deployed at U.S. Ports of Entry (POE) in the U.S. and in Canada. They provide non-intrusive screening of materials enclosed in large conveyances such as buses, cars, large tractor-trailer trucks, railcars, sea containers, and large 2,000-pound pallets. These systems have the ability to scan conveyances in one pass and provide quick reference images that can be stored and used for content analysis purposes. The scans display an image of the inside of various containers that appears similar to the examples below:



[1] E-Government Act of 2002, Pub. L. No. 107-347, § 208 (2002).
[2] 5 U.S.C. § 552a (a)(5), (e)(4).



In addition, large-scale NII imaging systems capture a photographic image of the conveyance's exterior to be stored in addition to the scanned image of the conveyance's interior, both of which may contain PII.

Small-scale NII imaging systems are deployed at U.S. air (including preclearance locations in Canada and the Caribbean), land, and sea POEs, and U.S. mail facilities handling international mail. They provide non-intrusive screening of luggage, packages, and flat mail. Small-scale NII imaging systems have the ability to provide quick reference images that can be stored and used for comparison purposes (e.g., checking the shapes, sizes, and other physical indicia for imported electronics to ensure the importation contains declared DVD players, instead of alarm clocks or other electronics that are not supposed to be in the package).

Mobile large-scale and small-scale NII imaging systems can be moved among POEs and checkpoints when necessary to meet CBP requirements. The trucks and mobile platforms have engines and are driven from one location to another as required. The NII computers are secured inside truck cabs or platform kiosks, securely fastened to the truck body or chassis. In addition, the cabs and kiosks are locked.

All CBP NII imaging systems permit CBP Officers to inspect merchandise and conveyances without the need for a more intrusive manual search. The individual driving the conveyance is usually not in the vehicle when the imaging system is employed, because it is usually safer to have a mobile NII platform scan over a stationary vehicle. NII systems provide images of material enclosed in cars, trucks, railcars, sea containers, personal luggage, packages, parcels, and mail. The images are stored on the hard drive associated with the NII system or written to a CD or other portable electronic media. If there are no anomalies (e.g., finding calculators when alarm clocks are claimed) found, the images are overwritten after a period of 30 days.

Vendors that provide NII imaging systems to CBP are required to provide the following storage capacity:

- Large-Scale NII Systems can export an image as a jpg file and copy the entire Image Data Set (IDS) to external media, which includes a CD, DVD, approved USB drive, and external hard drive. The System also can export images and copy Image Data Sets to an encrypted USB drive, such as an IronKey. An IDS is the collection of

electronic data gathered for a particular scan, including interior scans, exterior images, optical character recognition (OCR) scans that can read text (e.g., scanning the Automated Commercial Environment (ACE) electronic manifest cover sheet that is normally carried by conveyance drivers), license plate reader information, security camera live video capture, and metadata.

- Large-Scale NII Systems can store a complete IDS for a period of 30 days, or one (1) TeraByte of storage, whichever is reached first.
- Image Review – Last 50 Images and Automatic Image Archiving/Retrieval (25,000 images) for small-scale x-ray vans.

Inspection Process

Inspections at POEs are performed by CBP Officers. Although other government agencies have personnel and missions at POEs, only authorized CBP personnel operate these NII systems.

The inspection process for large cargo conveyances, begins with reviewing data from the cargo modules (Inbound and Outbound) of the Automated Targeting System (ATS), which provides an assessment of the risk associated with a particular shipment based on a variety of risk criteria.[3] Assisted by the ATS risk evaluation, the CBP Officer determines the need for additional inspection. Shipments deemed as high-risk and those randomly selected for inspection are scanned using large-scale NII imaging equipment for indications of contraband hidden inside. For small-scale items, all international luggage, mail, and parcels deemed high-risk are scanned. High-risk small-scale items are chosen based on several techniques including intelligence provided by the Office of Field Operations and anomalies detected by CBP Officers. Other small-scale items are scanned based on random selection.

Shipments showing no indications of anomalies are processed and released. Shipments indicating the presence of contraband may be scanned using a more sensitive or high-energy NII system, may undergo additional inspection with handheld small-scale NII equipment,[4] and may finally undergo a physical inspection of suspected areas identified by NII equipment to confirm whether illicit material is present. In cases in which contraband is found, CBP detains the shipment along with those transporting it for further investigation.

NII scanning equipment generally captures images by either slowly passing an arched scanner over a stationary conveyance (e.g., truck), or allowing the conveyance or shipment to

[3] DHS/CBP/PIA-006(b) - Automated Targeting System PIA Update (June 1, 2012), available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
SORN 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.

[4] Handheld small-scale NII equipment works in conjunction with large-scale NII equipment in inspecting cargo and conveyances at the nation's POEs.

pass through a stationary scanner. Images of the large-scale and small-scale NII equipment used for the scanning are available in the appendix.

In addition, photographic images of the conveyances are captured and may contain PII. These images are stored on the system or a disk along with a NII-generated image file number, a description of the contents, date, and time of scan. The location of the scan and vehicle identifier including license plate numbers can also be stored on the system or a disk. While most of the scanned images are deleted within 30 days, images that result in further investigation may be retained for law enforcement purposes, subject to retention reviews that occur both periodically and each time information is accessed, and may be retained as long as necessary for law enforcement purposes. The information collected and held within the NII systems is subject to retention requirements established by the National Archives and Records Administration (NARA). NARA's approved retention schedule specifies retention no longer than 30 days for NII records, with destruction or deletion of the NII records thereafter. This retention period applies to NII records not associated with a case file such as that belonging to a system of records; when NII records are associated with such a system of records (i.e., the Seized Assets and Case Tracking System known as SEACATS or TECS, a CBP system) the retention periods discussed in Section 5.1 apply.

The purpose of the NII Systems Program is to enable CBP to perform more effective and efficient inspections of cars, trucks, railcars, sea containers, personal luggage, packages, parcels, and flat mail. CBP owns and funds the project, which is operated pursuant to CBP's authority to conduct inspections at the border.[5] Conducting inspections with NII technology directly supports the CBP law enforcement mission, while also facilitating legitimate international travel, trade, commerce, and immigration. The NII Systems Program also supports several of DHS's core missions including preventing terrorism and enhancing security, securing and managing our borders, and enforcing and administering our immigration laws.

NII systems can collect PII about any individual whose PII appears on (or in) imported or exported shipments of goods, and is visible by photograph. Certain NII imaging systems collect scans and photos of the container or other conveyance contents. Additionally, the system collects and maintains the NII-generated image file number, container or conveyance identifiers (such as license plate numbers), a brief text description of container or conveyance contents, date and time of scan, and location of scan.

NII systems can also use OCR technology to read certain documents appearing on shipments that NII systems scan. However, a NII user cannot search the entire collection of all NII image data sets for the particular document information by a character string or similar search criteria. If a NII user thinks a particular shipment's IDS has some writing of interest on

[5] *See, e.g.*, 19 U.S.C. §§ 482, 1461, 1496, 1499, 1581-1582; *see generally United States v. Flores-Montano*, 541 U.S. 149 (2004).

the box's outside (e.g., importer's address), the user needs to know which IDS has that information before using OCR. This process is similar to suspecting a person of interest visiting a federal building on a given day, and looking at that day's visitor log.

Example

CBP receives a vessel manifest 24 hours prior to the cargo being loaded onto the vessel at the foreign port of departure/export. CBP processes this manifest information through ATS-Inbound to develop a risk score for the manifested cargo and its container. Upon arrival at the U.S port where the cargo is to be off-loaded (imported), CBP refers high-risk (based upon the score) and random cargo containers for additional screening using the NII technologies. If no anomaly within the shipment is detected in the NII image, the NII image is deleted after 30 days. If a CBP Officer identifies an anomaly within the scanned cargo container, this container is referred for physical inspection. A CBP Officer performing the physical inspection identifies any unmanifested items, and seizes or detains these items depending upon their status as prohibited (e.g., controlled substances, intellectual or cultural property), restricted (e.g., items requiring special documentation or licenses), or a misstatement as to the quantity. The report of inspection and any law enforcement action regarding seizure or detention is recorded into one of two CBP systems; TECS (DHS/CBP-011 - U.S. Customs and Border Protection TECS (73 FR 77778, Dec. 19, 2008)) or SEACATS (DHS/CBP-013 - U.S. Customs and Border Protection SEACATS (73 FR 77764, Dec. 19, 2008)), by the inspecting CBP Officer. As part of the administrative case processing for seizures, the electronic media from NII imaging and all corresponding documentation are referred to Fines, Penalties, and Forfeitures (FP&F) officers within CBP for the administrative processing of any law enforcement action. The FP&F Officer uses the NII images stored on the CD, DVD, or approved USB drive, and the data associated with the seizure in SEACATS or TECS to develop the seizure or penalty case resulting from the unmanifested cargo. The NII images at that point are subject to the retention policies set forth in SEACATS or TECS.

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 Homeland Security Act of 2002 created CBP as the single agency at the border with the authority to screen all persons, commercial vehicles, vessels, and containers for terrorist weapons and contraband. CBP's trade facilitation mission requires that this screening occur without significantly or negatively impacting the efficient movement of legitimate travelers and cargo across the border. The authority for NII includes, but is not limited to, 6 U.S.C. §§ 111, 203, 211, 212; Reorganization Plan Modification for the Department of Homeland Security, H.R. Doc. No. 108-32 (2003); 8 U.S.C. § 1357 (powers of immigration officers and employees); 18 U.S.C. § 831 (unlawful transactions in nuclear material); 19 U.S.C. §§ 482, 1401, 1461, 1496,

1499, 1581, 1582 (customs examination of persons, merchandise, baggage, and conveyances); Delegation from the Secretary of the Treasury to the Secretary of Homeland Security, Treasury Department Order No. 100-16, 68 FR 28322, 51868-70 (2003), codified at 19 CFR Part 0; 19 CFR 148.82(e); Delegation from the Secretary of Homeland Security to the Commissioner of U.S. Customs and Border Protection, No. 7010.3, May 11, 2006.

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

NII systems are not covered by a SORN, because the images in NII are not retrievable by reference to a name or unique identifier within NII systems. Further, the NII data are not searchable either by text searches (for character strings, e.g., license plate numbers of imported vehicles) or image searches (for biometrics, e.g., facial recognition of imported cadavers). Presently, NII data are not transmitted electronically to any other systems. Finally, NII images are stored on electronic media (such as a CD) identified by system-generated record locator numbers that are based only upon the date, time, and image number. In the case of seizure-related images (as in the SEACATS or TECS association described below), a separate data element can be retrieved. Specifically, location of the scan and vehicle ID including license plate numbers may be stored (i.e., added to the NII data file name, or linked to the NII data in a separate text file) for cases involving seizures.

However, when the NII images are referred for law enforcement action and entered into SEACATS (DHS/CBP-013 - U.S. Customs and Border Protection SEACATS (73 FR 77764, Dec. 19, 2008)) or TECS (DHS/CBP-011 - U.S. Customs and Border Protection TECS (73 FR 77778, Dec. 19, 2008)) as part of a case file, the NII images may be covered by the SORN for that system of records, as appropriate. As such, NII images become linked with a name or unique identifiers that are retrieved within these systems, including PII maintained in reports and records residing in the associated case file system of records. These systems provide electronic case management capability to support DHS law enforcement activities, and when appropriate the case status is updated to reflect the existence of images, maintained external to the system, to support the narrative remarks contained in the system.

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

Yes. The certification and accreditation (C&A) is completed with an authority to operate (ATO) granted on November 19, 2010. The ATO, in accordance with DHS and CBP policy, and in compliance with federal statutes, policies, and guidelines, provides that these systems are certified for a three-year period. A further extension to the ATO signed October 24, 2013, and expiring on January 3, 2014, provides NII authority to operate expiring to January 3, 2014; in the

interim, a new ATO is expected to be granted. The most recent date for a completed risk assessment is November 19, 2010.

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

Yes. NARA's approved retention schedule specifies retention no longer than 30 days for NII records, with destruction or deletion of the NII records thereafter.

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.

The information obtained during the process described in this PIA is not covered under the Paperwork Reduction Act (44 U.S.C. § 3501 et seq.).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

NII systems have the potential to collect PII about any individual whose PII both appears on (or in) imported or exported shipments of goods, and is visible by photography. Large-scale NII imaging systems collect images and photos of the container or other conveyance contents, the associated identifier number that may contain vehicle identifiers such as license plate numbers, a brief text description of container or conveyance contents, date and time of scan, and location of scan (NII systems without photography capability (i.e. small-scale NII) cannot collect this information). The tables below list the low-energy, medium-energy, and high-energy equipment used to collect the information.

Large-scale NII (low-energy)	Capabilities
Portal gamma-ray	radiological image; Pan-Tilt-Zoom (PTZ) camera or OCR snapshot; manifest scanning; entering notes
Mobile truck gamma-ray	radiological image; PTZ camera or OCR snapshot; manifest scanning; entering notes
Rail gamma-ray	radiological image; PTZ camera or OCR snapshot;

Large-scale NII (low-energy)	Capabilities
	manifest scanning; entering notes
Pallet gamma-ray	radiological image; PTZ camera or OCR snapshot; manifest scanning; entering notes
Mobile truck x-ray	radiological image; PTZ camera or OCR snapshot; manifest scanning; entering notes
Fixed x-ray	radiological image; PTZ camera or OCR snapshot; manifest scanning; entering notes
Z-Portal*	radiological image; PTZ camera or OCR snapshot; manifest scanning; entering notes

Large-scale NII (medium-energy)	Capabilities
Fixed x-ray	radiological image; PTZ snapshot; manifest scanning; entering notes
Mobile x-ray	radiological image; PTZ snapshot; manifest scanning; entering notes
Rail	radiological image; PTZ snapshot; manifest scanning; entering notes; printing summary report

Large-scale NII (high-energy)	Capabilities
Fixed x-ray	radiological image; PTZ or OCR snapshot; manifest scanning; entering notes
Mobile x-ray	radiological image; PTZ snapshot; manifest scanning; entering notes
Rail	radiological image; PTZ snapshot; manifest scanning; entering notes; printing summary report

* Occupants of a vehicle to be scanned by a Z-Portal have the option to either remain in the vehicle while the driver drives it through the portal, or exit the vehicle and have CBP

personnel drive it through the portal.

These data are collected on a computer that is integrated into the selected NII equipment. PII, in the form of vehicle or conveyance identification numbers, license plate numbers, operator or importer name, address and telephone number, may be collected from the photos that will be used by CBP to ensure that people, conveyances, and cargo entering or exiting the United States comply with all applicable U.S. laws. Specifically, data elements that may be stored on the NII system, some of which may contain PII, include:

- Body scans revealing persons attempting to enter the United States illegally, imported or exported cadavers, deceased persons, or persons otherwise concealed in a conveyance or container;
- Body scans of people who choose to remain in vehicles being scanned by a Z-Portal;
- Business name;
- Driver's license;
- Entry documentation;
- Vessel name, including registration number;
- Container number;
- Sender of the goods;
- Notes from officers related to a DHS/CBP action;
- Property description;
- Port of entry;
- Date of entry;
- Time of entry;
- Case number or seizure number;
- Type of violation or suspected violation;
- Date and place of violation or alleged violation;
- On-site disposition actions, such as whether a seizure was made, an item was detained, or inspection occurred;
- Memoranda; or
- Actions taken by DHS or CBP.

With respect to the biometric information listed above, these NII body scans have lower resolution that does not display a person’s skeletal structure (or metal implants within the body); but NII body scans may display items carried on the person (e.g., a handgun tucked into a waistband), or more macro body characteristics such as, for example, if a person has limbs missing. In the case of people who choose to remain in their vehicles during a Z-Portal examination of a vehicle, after being presented with the option to exit the vehicle by a CBP Officer prior to the vehicle being driven through the Z-Portal, the low level of x-rays used is within the health and safety limits allowable for members of the public. Signage (see Appendix)

at the port also advises the public of the low level of radiation for Z-Portal scans.[6] No signage exists for the times that the NII scans capture images of persons attempting to enter or exit the United States illegally while hidden in a shipment or conveyance.

NII systems sometimes electronically collects data from the Automated Commercial Environment (ACE) electronic manifest cover sheet that is normally carried by conveyance drivers; this cover sheet can be scanned and included as part of the IDS. CBP sometimes enters that cover sheet information into NII systems when there is a suspicion that the items being examined by NII pose some type of violation. For example, NII systems can use OCR to read the container number to tie a violation detected in the image to a particular shipment. Also, NII system operators can make observations about the item and enter that information into NII systems. If no contraband is found, the images and photos are rotated out of the computer as the space on the storage device reaches its capacity. The storage capacity varies with each NII system, but generally NII systems support data retention for 30 days. In the event of a positive scan, i.e., if contraband is found, the resulting seizure information is entered into SEACATS or TECS. SEACATS or TECS then assigns a seizure case number that references the NII internal associated tracking number for future reference. The scan image(s) and photo(s) are downloaded to a storage device and are submitted into evidence.

At this time, NII data are not transmitted electronically to any other systems. No information is received electronically by the NII systems from other systems. Information that must be disclosed for law enforcement purposes is stored on electronic media and entered into the TECS or SEACATS database by a CBP Officer. TECS or SEACATS information may be transmitted electronically or as printed materials to authorized DHS personnel, as appropriate.

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

The sources of the information are conveyances that pass through CBP operational areas, such as U.S. ports of entry, where NII systems are in use. 'Conveyances' include any vehicles or containers used to transport material or products, including mail, parcels, packages, etc. Information that pertains to potential operators or importers is separately maintained. NII systems have the potential to collect PII about any individual whose PII both appears on (or in) imported or exported shipments of goods, and is visible by photography. Images that contain PII may be retrieved by a record locator. Images of NII equipment are included in the appendix.

[6] For more information on x-rays go here:
http://www.ncrponline.org/Press_Rel/Commentaries/Comm_16_Press_Release.pdf

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

The NII system does not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

All CBP Officers must complete operator training before operating NII equipment. Among other skills, they are trained to recognize different types of images. The officer training, experience, and a comparison of the manifest listing the conveyance contents to the images obtained through use of NII systems all contribute to the accuracy of the identification process. If the officer identifies potential contraband, then further inspections occur to confirm the identification. The photos are visual records of the conveyances.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that information may be collected beyond the scope of CBP's missions.

Mitigation: Long-standing customs authorities allow for border searches to be performed with or without suspicion that the merchandise being searched may be in violation of U.S. law or may contain evidence of such a violation.[7] Such border search authority permits the physical examination of every container and conveyance presented at the border. However, CBP's mission also includes facilitating legitimate international trade. CBP uses NII systems to efficiently confirm that the contents of a container or conveyance match the declared goods described on the entry documents or to detect a violation. NII systems allow CBP to make these determinations without having to conduct time-consuming physical inspections of luggage and mail parcels or having to enter into conveyances, such as rail cars or shipping containers in order to both detect violations at the border and facilitate legitimate trade.

Also, all CBP Officers must complete operator training before operating NII equipment. Among other skills, they are trained to recognize different types of images. The officer training, experience, and a comparison of the manifest listing the conveyance contents to the images obtained through use of NII systems, when the only data elements are the images, all contribute to the accuracy of the identification process. If the officer identifies potential contraband, then further inspections occur to confirm the identification.

[7] *See United States v. Ramsey*, 431 U.S. 606 (1977). *See also* Act of July 31, 1789, ch 5, 1 Stat. 29.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CBP uses the information collected and maintained through the NII systems to carry out its law enforcement and national security mission. The images captured by the NII systems reveal the contents of a container and are used to inspect for contraband without having to enter into conveyances such as rail cars or shipping containers. If the use of an NII system and subsequent physical inspection results in a seizure, the captured images are stored on electronic media and transferred to CBP Officers for input into SEACATS administrative case processing, or TECS inspection and operational reports, for further law enforcement action.

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.

No. While some NII images (photos) may passively record PII, CBP does not employ special tools to search for and to analyze the NII systems data. The NII image data are not searchable either by text searches (for character strings, e.g., license plate numbers of imported vehicles) nor image searches (for biometrics, e.g., facial recognition of imported cadavers).

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

Only CBP Officers have direct access to NII. However, data from NII may be made available to other components within DHS on a need-to-know basis consistent with the component mission. Information may be shared within DHS to provide the DHS law enforcement community with information about potential threats. This objective supports CBP and DHS law enforcement and counter-terrorism missions. Components of DHS that have a need-to-know may have access to the relevant NII systems data.

The following DHS components may also have access to NII data that is entered into TECS:

- U.S. Immigration and Customs Enforcement;
- U.S. Citizenship and Immigration Services;
- U.S. Coast Guard;
- U.S. Secret Service;

- DHS Office of Biometric Identity Management;
- DHS Office of Inspector General and,
- Transportation Security Administration.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: NII images will be used in a manner inconsistent with the original purpose for which they were collected.

Mitigation: As set forth in the relevant SORNs, in furtherance of CBP's mission to facilitate legitimate international trade, CBP uses NII images and related photos to carry out its law enforcement and national security mission. The images captured by the NII systems are used to inspect for contraband without having to physically enter into conveyances, such as rail cars or shipping containers. To ensure that the images are accessed and used in a manner consistent with their original purpose of collection, NII images that support records governed by the SEACATS or TECS SORNs are saved on electronic media (such as CD, DVD, or approved USB drive), which is prominently marked "For Official Use Only" (FOUO). Such marked disks are stored in a locked, secure container in a secured area. Only users with prior authorization have access to the NII image CDs, DVDs, or approved USB drives.

Further, CBP vets and trains employees prior to giving the individual access to NII systems information or resources. This vetting is consistent with the types of information and resources that the individual needs to access to perform his or her duties. DHS/CBP policy requires the following: (1) components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels, and (2) no government employee or contractor shall be granted access to DHS/CBP systems without having a favorably adjudicated background investigation. Training is conducted for all CBP employees, as described in Section 8.2, below.

Privacy Risk: NII images will be misinterpreted and improperly used to the detriment of affected individuals.

Mitigation: All authorized users must take and successfully complete the CBP IT Rules of Behavior Training in addition to the mandatory Privacy Act training annually required for all CBP employees and contractors. Further training to accurately interpret the images is provided to all employees that use the equipment. Additionally, any adverse actions that result from the inspection provide the individual with the opportunity to access and amend the records through the procedures associated with the appropriate case file system of records.

Privacy Risk: There is a risk that NII photos, which may contain PII, are disclosed to unauthorized individuals within CBP.

Mitigation: CBP mitigates this privacy risk by storing photos in encrypted databases, or locked in file cabinets or locations that only authorized persons can access, in compliance with CBP policy. These physical protections supplement mandatory CBP employee privacy training, background investigations, and access-limiting protocols for handling NII systems data by CBP Officers.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

With regard to members of the public physically at a POE, signage is posted throughout POEs with large or small-scale NII systems that notify the public that NII image recording devices are in use. In POEs where Z-Portals are in use, signage at the port advises the public of the low level of radiation for Z-Portal scans, as people may choose to remain in their vehicles during Z-Portal examinations. At POE along the southern border, the warning signage is printed in English and Spanish. Please see the Appendix for sample signage. However, no signage exists for persons attempting to enter or exit the United States illegally while hidden in a shipment. This PIA provides notice to the general public as to the collection and use of NII images.

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

Individual members of the public do not have the opportunity or right to decline to provide information that NII images or photography may collect. Generally, the decision of whether to import or export articles to or from the United States is a matter with the discretion of the individual. NII image information must be provided pursuant to applicable statutes by all persons and cargo traveling through a U.S. port of entry where NII systems are in use. The only legitimate means of declining to provide the subject information is to not seek to enter, transport, ship, or mail goods/merchandise at or through a POE or other CBP operational area, or to choose not to remove such goods or merchandise from a POE or other CBP operational area. In addition, NII systems scan and collect images of outbound conveyances departing the United States for foreign destinations.

Because the submission of information is a pre-requisite for inbound and outbound travel into or out of the U.S., any restrictions on the use and sharing of accessed information by CBP is subject to limitations outlined in the Privacy Act, Trade Secrets Act, and the System of Records Notices (e.g., TECS or SEACATS) governing case files with which the NII images are

associated. Consent to store or use this information must be done in accordance with the above legal requirements, but individuals do not have the right or opportunity to provide consent for specific uses.

Inasmuch as the NII systems utilized at the POEs (or at other CBP operational areas) are continually in use, there is effectively no mechanism for an individual to decline to provide information, opt out of the project or decline to consent to the uses of the information. The only way for an individual to avoid the program is to not seek to enter, transport, ship, or mail goods/merchandise at or through a POE or other CBP operational area, or to choose not to remove such goods or merchandise from a POE or other CBP operational area.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware that their information may be recorded in NII images and photographs.

Mitigation: In order to provide notice to the individual members of the public importing or exporting goods into or out of the United States – in addition to the publication of this PIA – signs are prominently posted throughout a POE with NII systems that notify the public that NII imaging devices are in use. In POEs where Z-Portals are in use, signage at the port advises the public of the low level of radiation for Z-Portal scans as people may choose to remain in their vehicles during a Z-Portal examination of a vehicle. At POEs along the southern border, the warning signage is printed in English and Spanish. Please see the Appendix for example signage. However, no signage exists for persons attempting to enter or exit the United States illegally while hidden in a shipment during NII scanning.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Most of the photos and scan images are deleted within 30 days, to allow sufficient time to review and to decide if law enforcement action is necessary. If a photo or scan image is referred for law enforcement action (e.g., investigation, administrative action, or a judicial proceeding), then the NII image is associated with information about the merchandise and/or importer and/or exporter. This information (about the importer and/or exporter and merchandise, as well as the NII image) is entered as a case into SEACATS, where it is retained until the conclusion of the law enforcement action, plus five years.[8] If the applicable statute of limitations period for bringing a cause of action to address the action ends before the resolution of the legal matter, the records are retained for two years beyond the expired statute of limitations period.

[8] DHS/CBP-013 System of Records Notice for SEACATS, December 19, 2008, 73 FR 77764, 77767

When the associated image information is entered into TECS, the retention period in the TECS database is 75years from the date of the collection of the information or for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).[9]

The National Archives and Records Administration (NARA) has approved a record retention and disposition schedule (schedule) for the NII systems. NARA's approved retention schedule specifies retention no longer than 30 days for NII records, with destruction or deletion of the NII records thereafter. This retention period applies to NII records not associated with a case file such as that belonging to a system of records; when NII records are associated with such a system of records (i.e., SEACATS or TECS), the retention periods discussed above apply.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data may be retained too long, which reduces the relevance and timeliness of the data.

Mitigation: To ensure that data is kept only for the shortest time period necessary, non-significant (i.e., not related to an incident or event not requiring a SEACATS or TECS case file) NII images and photos are routinely erased after storage capacity has been reached, typically 30 days. Unless a particular incident or event is identified and a backup (CD, DVD, approved USB drive, or external hard drive) copy is made, more recent recordings overwrite previous data when the storage device reaches its 90-day capacity. Electronic media containing NII images that suggest the need for law enforcement action (e.g., a potentially counterfeit mark) are associated with a case file governed by the TECS SORN or SEACATS SORN both of which have defined retention periods. In all cases, media for which the retention period passes are erased and reused and/or destroyed and disposed of in accordance with approved procedures.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

DHS may use this information in support of its mission responsibilities, including in situations when NII records are relevant for evidentiary purposes, such as when smuggled contraband is discovered through the use of NII equipment. As part of the law enforcement mission of CBP, images – as well as case file notes explaining the image – from NII systems

[9] DHS/CBP-011 TECS System of Records Notice for December 19, 2008, 73 FR 77778

may be shared with other agencies to assist with their law enforcement investigations or intelligence operations. When an image from NII is associated with a case file in SEACATS or TECS, those images may be shared along with other case file information covered in that system of records consistent with the Privacy Act of 1974 and the routine uses in the applicable SORN, as authorized by the CBP Privacy Officer.

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

The TECS and SEACATS SORNs (published at 73 FR 77778 and 73 FR 77764, respectively) 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 mission including ensuring the security of the United States by deterring terrorists from smuggling weapons and explosives across the border, as well as stemming the tide of illegal drugs.

Also, as discussed, the NII system itself is not covered by a SORN, because the scanned images are not retrievable by reference to a name or other PII within the NII system (for images not associated with cases covered by TECS or SEACATS).

6.3 Does the project place limitations on re-dissemination?

NII images that are not associated with a system of records may be shared when the requesting law enforcement agency has an official need to know and agrees to limit re-dissemination of the images. When NII images are associated with a system of records, authorization to share information with an external agency is subject to approval by the CBP Privacy Officer, insofar as the request and use are consistent with the Privacy Act, the published routine uses for the appropriate SORN, and the receiving agency's agreement to be restricted from further unauthorized sharing of the information. The receiving agency's acceptance and use of the shared information is conditioned on (1) the receiving agency's use being consistent with the purpose for collection, (2) the sharing being consistent with a statutory or published routine use, and (3) the receiving agency's acceptance of the restriction barring unauthorized dissemination outside the receiving agency.

These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

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

NII images associated with a system of records that are shared outside of the Department are tracked through the use of the DHS-191, Accounting of Disclosure Form. CBP users of NII

systems prepare a DHS-191 form each time they share NII information covered by a system of records outside of DHS. CBP and DHS share information from NII in accordance with the language of a letter of authorization, which facilitates the sharing of a particular record from NII in response to a request for assistance from another agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information may be shared under inappropriate circumstances.

Mitigation: When sharing information with third parties, the same limitations on the use of the information that are in place for CBP and DHS also apply to the outside entity. Access to CBP data is governed by "need to know" criteria that require that the receiving entity demonstrate the need for the data that is consistent with the use for which it was originally collected before the NII images are disseminated. Likewise, with regard to security of the information and accountability of the personnel using it, the receiving entity must provide assurances that the data will be safeguarded in a manner consistent with CBP/DHS policy and practice and that no disclosure of any shared data will occur without the express prior written permission of CBP. In the event that a recurring sharing arrangement is contemplated between CBP and a federal agency outside DHS, CBP develops a written arrangement (e.g., MOU) that specifies with particularity all terms and conditions that govern the use of the functionality or data, including limitations on use. CBP periodically reviews the written arrangement and verifies that the outside entity conforms to use, security, and privacy considerations before the information's release.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals may request information about their records contained in NII systems through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and, whenever those records contained in NII systems are also associated with a system of records as described in Section 1.2, the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)).

Generally, NII systems do not record or retrieve information by personal identifiers, so it is difficult for an individual to find and view a particular NII IDS. IDS are retrieved by date/time or NII-generated image file number. Additionally, an NII IDS is only stored for a maximum of 30 days. The NII IDS is then recorded over, which limits the amount of time an individual has to access his or her information. Accordingly, an individual wishing to access his or her

information from NII systems should provide the time, day, entry number, and specific POE to find the information, or other identifying information that will assist CBP in locating the requested record.

Individuals seeking notification of and access to any record contained in NII 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/.

Individuals can submit a Freedom of Information Act (FOIA) request using procedures outlined on the CBP web page at: https://foia.cbp.gov/Request/palLogin.aspx.

To the extent a record is covered by the Privacy Act as part of a case, information may be exempt from individual access or amendment provisions of the Privacy Act because access to the data in NII systems could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. In other cases, however, individuals may be able to gain access to the data pertaining to them. Determinations regarding the granting or denial of access are made once the request is received by the CBP Privacy Officer who forwards it, if necessary, to the data-owning office. Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request does not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with CBP procedures.

Because of the law enforcement nature of NII, the Secretary of the Department of Homeland Security has exempted the systems of records associated with NII from the notification, access, and amendment requirements of the Privacy Act.[10] Because of the law enforcement purposes for which information is collected, individuals do not have direct access to NII systems or the data contained therein.

[10] SEACATS (DHS/CBP-013 - U.S. Customs and Border Protection SEACATS (73 FR 77764, Dec. 19, 2008)) or TECS (DHS/CBP-011 - U.S. Customs and Border Protection TECS (73 FR 77778, Dec. 19, 2008)).

NII overwrites an IDS generally 30 days after the scan. In cases requiring law enforcement action, the information may be retained longer as described in Section 5.1. NII systems also destroy the information pursuant to the retention policies discussed in 5.1.

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

The NII system records live action images. No procedures exist to edit, correct, or amend the recorded information, aside from copying images of events needing law enforcement follow-up to a CD, DVD, or approved USB drive. However, NII images associated with a case file follow the access and amendment procedures associated with that system of records. If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue
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 the NII system are informed that they may submit a request through the procedures in 7.1 and 7.2, above. Individuals seeking NII records contained in applicable CBP systems of records must submit requests which conform to the Privacy Act regulations set forth in 6 C.F.R. Part 5, in accordance with the system of records notices for those systems (the TECS SORN, 73 FR 77778 (Dec. 19, 2008) and SEACATS SORN, 73 FR 77764 (Dec. 19, 2008)).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Due to the law enforcement nature of this system, and the fact that recordings cannot be altered, individuals may not correct or amend the recordings.

Mitigation: The system operates as a passive observer, creating records of import and export activity at POEs with NII systems. As such, individual participation by the public seeking to import or export goods into or out of the United States is not elective; the only way to decline participation is to choose not to enter, transport, ship, or mail goods/merchandise at or through a POE or other CBP operational area, or to choose not to remove such goods or merchandise from a POE or other CBP operational area. CBP provides awareness of the system and the creation of recordings through onsite signage and the publication of this PIA. Because the records are a memorialization of events as they occur, they cannot be amended or corrected. However, limited

redress, in the form of access, is available through requests as described in Sections 7.1 and 7.2. When an NII record is associated with a case file in another system of records, individuals may seek redress through the procedures for that system of records.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

Files are proprietary, meaning that the non-photo (i.e., radiographic), NII images can only be viewed on an NII workstation, which may be accessed only from within a secure CBP facility. Multiple forms of authentication are required before entering the facility, to include badges, locked doors, keyed entries, etc. Users of NII systems are required to log into a CBP workstation using a CBP hash ID and valid password, and are then also required to log into the NII system itself. Additionally, authorized users of NII systems must successfully complete training as described in Sections 3.4 and 8.2.

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

All CBP officers and Border Patrol agents receive training at federal facilities for their specific role and all CBP employees are required to take annual "CBP IT Security Awareness and Rules of Behavior Training" through the online DHS Virtual Learning Center to gain access to the CBP network, systems, or data. All CBP employees and contractors must also complete mandatory Privacy Act training annually.

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

NII system user access is restricted to certain designated CBP Officers and other similarly authorized CBP personnel with a need to know. Access to particular NII data is based upon the user's role.

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?

No routine sharing of recorded image and photo files exists. However, in the event that a recurring sharing arrangement between CBP and an agency outside DHS is contemplated, CBP

develops a written arrangement (e.g., Memorandum of Understanding) to establish the terms of use and security for the exchanged data. The written arrangement specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. CBP periodically reviews the written arrangement and verifies that the outside entity conforms to use, security and privacy considerations before information was released.

Responsible Officials

Laurence E. Castelli,
CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

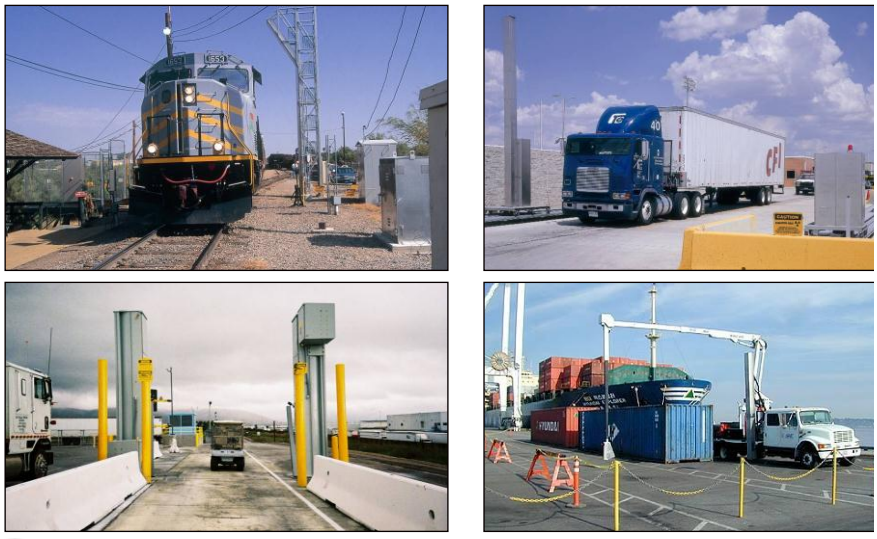
_____

Karen Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Signage for Z-Portal

Gamma-ray Systems

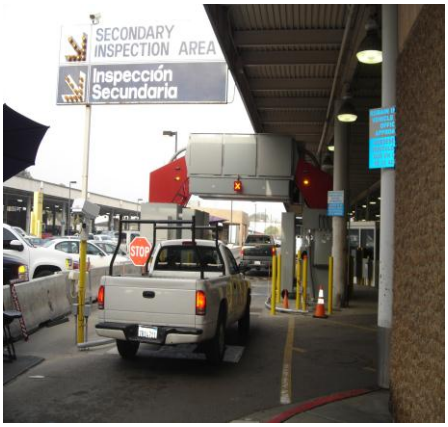


U.S. Customs and Border Protection

High Energy Fixed X-ray Systems

U.S. Customs and Border Protection

Portal System



U.S. Customs and Border Protection

Mobile Equipment

U.S. Customs and Border Protection

Small-Scale NII Technology

101
X-RAY VAN

LASER RANGE FINDER

PORTABLE CONTRABAND DETECTOR – "BUSTER"

LARGE BAGGAGE SYSTEM

FIBER OPTIC SCOPE

SMALL BAGGAGE SYSTEM

TOOL TRUCK