Privacy Impact Assessment for the

E-Commerce "Section 321" Data Pilot

DHS/CBP/PIA-059

September 26, 2019

Contact Point

Laurie Dempsey

Director

Intellectual Property Rights (IPR) and E-Commerce

Policy and Programs Division

(202) 615-0514

Reviewing Official

Jonathan Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) is conducting a voluntary test to collect certain advance data related to shipments potentially eligible for release under Section 321 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1321 ("Section 321"). Section 321 provides for an administrative exemption from duty and taxes for shipments of merchandise (other than bona-fide gifts and certain personal and household goods) imported by one person on one day having an aggregate fair retail value in the country of shipment of not more than $800. Pursuant to this test, participants will electronically transmit certain data elements pertaining to these shipments to CBP in advance of arrival. CBP is conducting this test to determine the feasibility of requiring advance data from different types of parties and requiring additional data that is generally not required under current regulations in order to effectively identify and target high-risk shipments in the e-commerce[1] environment. CBP published a Notice in the Federal Register on July 23, 2019, announcing the pilot.[2] CBP is publishing this new Privacy Impact Assessment (PIA) to provide notice of information collection requirements for the Section 321 Data Pilot, and to assess the privacy risks of its collection and use of personally identifiable information under this pilot.

Overview

Section 321 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1321 ("Section 321") authorizes CBP to provide an administrative exemption to admit free from duty and tax shipments of merchandise (other than bona-fide gifts and certain personal and household goods) imported by one person on one day having an aggregate fair retail value in the country of shipment of not more than $800.[3] CBP regulations provide that, subject to the conditions in 19 CFR § 10.153, the port director shall pass free of duty and tax any shipment of merchandise imported by one person on one day having a fair retail value in the country of shipment not exceeding $800, unless there is a reason to believe the shipment is one of several lots covered by a single order or contract, and was sent separately for the express purpose of securing free entry or of avoiding compliance with any pertinent law or regulation.[4]

Prior to the enactment of the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA)[5] the Section 321 exemption applied only to shipments valued at less than $200. TFTEA increased the administrative exemption (the so-called "de minimis" exemption) value from $200 to $800. Beginning March 10, 2016, this change permitted many articles valued at $800 or less

[1] CBP defines e-commerce as high-volume, low-value shipments entering the port limits of the United States.
[2] 84 Fed Reg. 35405 (July 23, 2019).
[3] 19 U.S.C. § 1321(a)(2)(C).
[4] 19 CFR § 10.151.
[5] Pub. L. 114-125, 130 Stat. 223 (Feb. 24, 2016).

imported by one person on one day to become eligible for duty- and tax-free entry under Section 321 and its implementing regulation, 19 C.F.R. § 10.151.

TFTEA's change to the de minimis value, however, caused a dramatic increase in the volume of shipments making use of de minimis entry procedures. These procedures provide fewer data elements for CBP to use to effectively identify and target high-risk shipments, including for narcotics, counter-proliferation, and health and safety risks. The dramatic increase in shipments has left CBP with less information about a greater number of shipments.

The increasing use of new and changing industry business models, particularly in the e-commerce environment, further exacerbates this information gap. Entities receiving goods in the United States, which CBP previously believed to have limited financial interest in a shipment, are now critical players with increasing influence in how low-value goods move around the world. This shift in the roles of parties to the transaction has not been accompanied by a change in responsibilities from a regulatory or policy perspective. Moreover, the advent of just-in-time delivery, along with contract manufacturing and online payment processing, has given merchants more flexibility and greater access to markets once limited by location. Free trade agreements have also allowed new routes for goods from all over the world to cross borders more easily.

CBP is concerned that the proliferation of new and changing business models, particularly in the e-commerce environment, and the increase in small packages, is permitting bad actors to operate with relative impunity.

Data Collection Gaps and Risks

CBP has broad authority to collect advance data and inspect cargo crossing the border for compliance with the customs laws, including those related to health, safety, and other risks pursuant to various statutory authorities.[6] Currently, CBP requires the electronic transmission of certain information relating to commercial cargo prior to its arrival in the United States, regardless of the mode of transportation.[7] For air, regulations also require carriers or other eligible parties to transmit a subset of the data earlier in the process (i.e., as soon as practicable, but no later than prior to loading the cargo into an aircraft).[8] For shipments arriving by vessel, CBP regulations require importers and carriers to submit additional data, in addition to the data required by the Trade Act regulations, before the cargo is brought to the United States.[9]

CBP requires fewer data elements for informal entry. Informal entry is generally available for shipments not exceeding $2,500, and thus is generally available for shipments that qualify for Section 321. There are a variety of means for making informal entry, depending on the status of

[6] See, e.g., 6 U.S.C. 211(c) and (g); 19 U.S.C. 482, 1431, 1461, 1499, 1589a, 1595a; see also 19 CFR 162.6.
[7] See 19 CFR 4.7 (vessel), 122.48a (air), 123.91 (rail), and 123.92 (truck).
[8] See 19 CFR 122.48b(b)(1).
[9] See 19 CFR part 149 (the Importer Security Filing or ISF regulations).

the merchandise; CBP regulations prescribe certain forms that can be used based upon such status. Where the value of shipment does not exceed $800 and the shipment satisfies Section 321 requirements, informal entry may be made by presenting the bill of lading or a manifest listing each bill of lading (except for mail importations or in the case of personal written or oral declarations).[10] The information required to be filed for a Section 321 release—or "release from manifest"—includes: (1) country of origin of the merchandise; (2) shipper name, address, and country; (3) ultimate consignee name and address; (4) specific description of the merchandise; (5) quantity; (6) shipping weight; and (7) value.[11]

In the e-commerce environment and with the advent of new data elements, traditionally regulated parties, such as carriers, are unlikely to possess all of the information relating to a shipment's supply chain. Specifically, the shipment originator, final destination, and package contents are often unknown. While CBP receives some advance electronic data for Section 321 shipments from air, rail, and truck carriers (and certain other parties in limited circumstances) as mandated by current regulations, the transmitted data often does not adequately identify the entity causing the shipment to cross the border, the final recipient, or the contents of the package. Consequently, CBP may not receive any advance information on the entity actually causing the shipment to travel to the United States, such as the seller or manufacturer. For a de minimis entry, the closest data field for that would be the "shipper," but that likely is not the actual seller but rather a party that arranges for or handles shipping for a host of entities. Even on a formal entry, the seller in an e-commerce transaction may or may not be identified. What is required on a formal entry is the "manufacturer ID," which usually is the "invoicing party."[12] Thus, this could be the actual seller, or could be an agent that is providing invoicing services.

This data pilot seeks to collect information from a variety of participants, including e-commerce participants that have previously operated outside of the customs clearance process. Entities such as marketplaces, consolidators, fulfillment centers, and carriers operated under a much different context prior to the growth in online, direct-to-consumer sales.

Collection from a variety of entities through this pilot seeks to capture information often not transmitted to CBP. Described below are some common business model scenarios and the data challenges that they present. This list is by no means exhaustive but is intended to show the importance of certain entities under Section 321 releases. Notably, many businesses today use a combination of these models.

---

[10] 19 CFR § 143.23(j).
[11] 19 CFR § 143.23(k).
[12] The entry summary documentation, as required for entry under 19 CFR § 142.3, must be on the CBP Form 7501, or its electronic equivalent. *See* 19 CFR § 142.11. CBP Form 7501 Instructions instruct persons completing CBP Form 7501 (providing the entry summary) to report the manufacturer ID code according to "the invoicing party or parties (manufacturers or other direct suppliers)." *See* https://www.cbp.gov/sites/default/files/assets/documents/2016-Sep/CBP%20Form%207501_Instructions%20%28Fixed%20Links%2009-07-2016%29.pdf.

Proprietary Websites

One business model that has proved successful in e-commerce transactions consists of websites that sell branded goods from a U.S. or foreign seller, or even a foreign manufacturer, directly to a consumer through a website. While this business model appears relatively simple, problems may arise, as these websites are easy to set up anonymously, masking the identity of the seller of counterfeit goods. Express Consignment Carriers (such as FedEx, UPS, etc.), brokers, freight forwarders, and other entities pack and ship the product through U.S. Customs. Where the seller is directly sending through one of these entities, entities that pack and ship the products are often the best suited to inform CBP of the product's origin and the shipment originator, since for Section 321 entries, the consumer can be listed as the buyer/importer of record. Information about the website owner and/or foreign seller or foreign manufacturer is unlikely to appear on the manifest.

Third-Party Websites

Several third-party websites operate a platform-as-a-service model, providing businesses a platform to sell merchandise directly to consumers. The sellers and manufacturers may be foreign or domestic, and a portion of the transaction value is often paid to the platform provider. While this provides many benefits for consumers, it has introduced ambiguity as to the authenticity and safety of the merchandise being sold and increased the informational distance between the consumer and shipment originator.

Fulfillment Center

Another business model is the use of fulfillment centers, which are warehouses in the United States used for a variety of reasons, including possible repackaging, storage, and distribution. In this model, a foreign business may use a website (proprietary or third party) to advertise and sell a product to a consumer. This foreign business packages the product for shipment to the United States, where it is delivered by a carrier to a distribution warehouse within the United States for repackaging and/or storage, if the item is not yet sold. Once the item is sold and repackaged at the distribution center, a courier or USPS delivers the item to the consumer. CBP often lacks visibility into the final consumer, since the shipment can begin movement without a buyer. There are also additional opportunities for contraband to enter the supply chain due to multiple changes of custody. Further, there are additional information gaps when the product arrives in the United States prior to sale to a domestic consumer.

Foreign Fulfillment Center

Businesses may also use foreign fulfillment centers to package and ship a product to a U.S. consumer. In this model, foreign entities deliver their goods to a foreign distribution warehouse, outside of the ownership of the original manufacturer or producer. An online marketplace lists those products on their website. When a product is sold, the foreign distribution center packages

the product for shipment via a carrier, courier, or international mail, and delivers the item to the consumer. Under this business model, CBP often lacks visibility into the shipment originator.

Foreign Consolidation

There is increasing use of foreign consolidation in the e-commerce environment. Regardless of how a product is sold (through a proprietary website, third-party website, fulfilment center, or combination), many entities use foreign consolidators to ship the product to the United States, or to a foreign fulfilment center prior to shipment to the United States. For this business model, U.S. or foreign entities list their product online. A foreign logistics provider aggregates shipments from a variety of firms often under a master bill for delivery to a U.S. logistics provider. The U.S. logistics provider unbundles the shipments in preparation for shipment to the consumer or fulfillment center. Under this business model, CBP does not see the shipment originator or final deliver to party.

Pilot Overview

To address the gaps described above, CBP issued a Federal Register notice on July 23, 2019,[13] seeking volunteers to test the collection of certain advance data related to shipments potentially eligible for release under Section 321 of the Tariff Act of 1930, as amended. CBP is seeking participation from stakeholders in the e-commerce environment, including carriers, brokers, and freight forwarders, as well as online marketplaces. There are no restrictions with regard to organization size, location, or commodity type. However, participation is limited to those parties with sufficient information technology infrastructure and support. Specifically, participants, or an authorized carrier or broker, must have the technical capability to electronically submit data to CBP and to receive messaging responses via a point-to-point connection with CBP. Participants who establish a new point-to-point connection with CBP will need to sign an Interconnect Security Agreement (ISA) or amend their existing ISA, if necessary, and adhere to DHS information security policies.

Pursuant to this test, participants will electronically transmit certain data elements pertaining to these shipments to CBP in advance of arrival. CBP is conducting this test to determine the feasibility of requiring advance data from different types of parties and requiring additional data that is generally not required under current regulations in order to effectively identify and target high-risk shipments in the e-commerce environment.

Participants may include carriers, brokers, and freight forwarders, as well as non-traditional CBP partners, such as online marketplaces. Online marketplaces generally have detailed information regarding Section 321 shipments, including information relating to the party causing the product to travel to the United States, the final recipient in the United States, and detailed descriptions and pictures of the contents of the shipment. Online marketplaces may also assign

[13] 84 Fed Reg. 35405 (July 23, 2019).

unique identifiers to sellers or develop their own known seller programs. This test will enable CBP to assess the ability of online marketplaces to transmit information to CBP that enables CBP to better use resources in inspecting and processing these shipments and better understand the operation of online marketplaces.

Additionally, CBP is testing whether the transmission of additional advance data, beyond the data elements currently required for shipments arriving by air, truck, or rail, will enable CBP to more accurately and efficiently target Section 321 shipments. Pursuant to this test, participants will provide information that identifies the entity causing the shipment to cross the border, the ultimate recipient, and the product in the shipment with greater specificity, in advance of the shipment's arrival. CBP will test the feasibility of using the additional data elements, transmitted by multiple entities for a single shipment, to segment risk. For example, CBP may compare a picture of the product (transmitted by an online marketplace) to an x-ray image of the package (transmitted by the carrier) to determine if the picture of the product and x-ray image match. In sum, the pilot will enable CBP to determine if requiring additional data and involving non-regulated entities will enable CBP to address the threats and complexities resulting from the vast increase in Section 321 shipments, while facilitating cross-border e-commerce.

The voluntary pilot will begin upon publication of this Privacy Impact Assessment and run for approximately one year.

Pilot Concept of Operations

Pilot participants will electronically transmit certain data elements specified below in section 2.1 (Data Elements) in addition to other data elements, as available and at the participant's discretion. CBP must receive the data elements prior to the shipment's arrival in the United States. Participants may electronically transmit the requested information through an existing point-to-point connection with CBP. Alternatively, participants may authorize a carrier or broker participating in the pilot who has an existing point-to-point connection with CBP to transmit the information on their behalf. CBP will respond to the data transmissions with a confirmation of receipt and will use the transmitted information to conduct risk assessments. Risk assessment for each shipment will be based on multiple transmissions, as each transmission can be from different parties providing different data elements at various stages in the supply chain. Messages will be maintained in the Automated Targeting System (ATS).

The Section 321 Data Pilot will not affect any current requirements, and CBP is not waiving any regulations for purposes of the pilot, including all the regulations pertaining to the provision of advance data cited above, such as the Air Cargo Advance Screening (ACAS) and Importer Security Filing (ISF) regulations. All existing Trade Act of 2002 requirements and all manifest requirements continue to apply. Additionally, CBP will not use the information transmitted pursuant to the pilot for entry or release purposes, and pilot participants cannot rely on information transmitted through the pilot for entry or release purposes.

Future State

CBP will evaluate pilot results and determine whether to extend the duration of the pilot and/or expand the pilot to include additional participants. Additionally, CBP will assess whether additional mandatory advance reporting requirements are necessary in the e-commerce environment.

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?

CBP has broad authority to collect advance data and inspect cargo crossing the border to determine compliance with U.S. law, including for health, safety, and other risks pursuant to various statutory authorities. *See, e.g.*, 6 U.S.C. § 211(c) and (g); 19 U.S.C. §§ 482, 1415, 1431, 1461, 1499, 1589a, 1595a; *see also* 19 CFR §§ 122.48a, 122.48b, 123.91, 123.92, and 162.6.

This pilot is conducted pursuant to 19 CFR 101.9(a), which authorizes the Commissioner to impose requirements different from those specified in the CBP regulations for the purposes of conducting a test program or procedure designed to evaluate the effectiveness of new technology or operational procedures regarding the processing of passengers, vessels, or merchandise. As noted above, participation in this test is voluntary, and CBP has published a Notice in the Federal Register seeking participation from stakeholders in the e-commerce environment, including carriers, brokers, freight forwarders, and online marketplaces.

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

CBP maintains the Section 321 Data Pilot information in ATS in accordance with DHS/CBP-006 Automated Targeting System SORN.[14] The ATS SORN covers CBP's comparison of traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting rules and assessments to identify individuals and cargo that require additional scrutiny. In addition, the Import Information System (IIS)[15] SORN covers CBP's collection of import information data.

In addition, CBP is in the initial stages of drafting a new system of records notice specific to Cargo Security Records, which will cover the Section 321 Data Pilot and all records that CBP maintains for cargo security purposes.

[14] 77 FR 30297 (May 22, 2012).
[15] 81 FR 48826 (July 26, 2016).

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

Yes. The Section 321 Data Pilot was granted an Authority to Test (ATT) on July 31, 2019, with an expiration date of July 31, 2020. The Federal Information Processing Standards (FIPS) determination for this system is moderate for confidentiality, integrity, and availability.

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

CBP is in the process of creating a NARA-approved records retention schedule for records generated as part of the e-Commerce Section 321 pilot. The CBP Records and Information Management Division is working with the program and system owner to develop a new schedule. CBP will retain records created as part of the Section 321 Data Pilot as permanent records in ATS pending a NARA-approved records retention schedule.

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. § 3510). The Section 321 Data Pilot initially will collect information from nine volunteers from the trade community and thus does not meet the PRA requirement for collection as there are fewer than ten participants. If CBP deems the pilot successful, CBP will expand participation and update the PIA at that time.

Section 2.0 Characterization of the Information

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

Participants in the Section 321 Data Pilot will transmit certain information for Section 321 shipments that are destined for the United States and for which the participant has information. Although much of this information is data that CBP already collects off the manifest, bill of lading, or other forms depending on the mode of transportation, it is often presented in a way that does not provide CBP with a full and accurate view of who is causing the shipment to move, the shipment's contents, and its final destination. Collecting information directly from online marketplaces and piecing together additional data from other e-commerce actors (e.g., carriers,

brokers, and freight forwarders) as the shipment makes its way through the supply chain is key in addressing this challenge. Pilot participants are encouraged to transmit this information via a separate point-to-point connection with CBP and as far in advance as possible to help CBP segment risk prior to arrival in the United States. To further assist CBP in segmenting risk, participants may also provide the following seven new data elements: Known Carrier Customer Flag, Known Marketplace Seller Flag, Marketplace Seller Account Number/Seller ID, Product Picture, Link to Product Listing, Listed Price on Marketplace, and Buyer Account Number.

Certain data elements are mandatory for all who volunteer to participate in the pilot. The required data elements differ slightly depending on what entity is transmitting the data. In general, the required data relates to the entity initiating the shipment (i.e., the entity causing the shipment to cross the border, such as the seller, manufacturer, or shipper), the product in the package, the listed marketplace price, and the final recipient (i.e., the final entity to possess the shipment in the United States). The data elements are as follows.

1. All participants: All participants, regardless of filer type, must electronically transmit the following elements:
    a. Originator Code of the Participant: CBP will email participants a unique originator code at the onset of their pilot engagement and the participant will submit the originator code with each filing to confirm their identity;
    b. Participant Filer Type (e.g., carrier or online marketplace);
    c. One or more of the following:
        i. Shipment Tracking Number;
        ii. House Bill Number;[16] or
        iii. Master Bill Number;[17]
    d. Mode of Transportation (e.g., air, truck, or rail).
2. Participating carriers: In addition to the data elements listed above in paragraph 1, participating carriers must also electronically transmit the following data elements:
    a. Shipment Initiator Name and Address (e.g., the entity that causes the movement of a shipment, which may be a seller, shipper, or manufacturer, but not a foreign consolidator);
    b. Final Deliver to Party Name and Address (e.g., the final entity to receive the shipment once it arrives in the United States, which may be a final purchaser or a warehouse, but not a domestic deconsolidator);

[16] House waybill (HAWB) is the number for each shipment within a consolidated shipment
[17] Master waybill (MAWB) is the number that is generated by the inbound carrier for a consolidated shipment.

c. Enhanced Product Description (e.g., a description of a product shipped to the United States more detailed than the description on the manifest, which should, if applicable, reflect the advertised retail description of the product as listed on an online marketplace);

d. Shipment Security Scan (air carriers only) (e.g., verification that a foreign security scan for the shipment has been completed, such as an x-ray image or other security screening report);

e. Known Carrier Customer Flag (e.g., the carrier may electronically submit an indicator that identifies a shipper as a repeat customer that has consistently paid all required fees and does not have any known trade violations);

3. Participating online marketplaces: In addition to the data elements listed above in paragraph 1, participating online marketplaces must electronically submit the following data elements:

a. Seller Name and Address (e.g., an international or domestic company that sells products on marketplaces and other websites), and, if applicable, Shipment Initiator Name and Address;

b. Final Deliver to Party Name and Address;

c. Known Marketplace Seller Flag (e.g., an online marketplace may electronically submit an indicator provided by a marketplace that identifies a seller as an entity vetted by the marketplace and with no known trade violations);

d. Marketplace Seller Account Number/Seller ID (e.g., the unique identifier a marketplace assigns to sellers);

e. Buyer Name and Address, if applicable (e.g., the purchaser of a good from an online marketplace; this entity is not always the same as the final deliver to party);

f. Product Picture (e.g., picture of the product presented on an online marketplace), Link to Product Listing (e.g., an active and direct link to the listing of a specific product on an online marketplace), or Enhanced Product Description; and

g. Listed Price on Marketplace (e.g., the retail price of a product that a seller lists while advertising on an online marketplace. For auction marketplaces, this price is the price of final sale).

Different entities may transmit different data elements for the same shipment. In addition to the above required data elements, participants may voluntarily provide the following optional data elements:

- Harmonized Tariff Schedule (HTS)[18] Number;
- Retail Price in Export Country;
- Shipper Name;
- Shipper Address;
- Shipper Phone Number;
- Shipper Email Address;
- Shipment Initiator Phone Number;
- Consignee Name;
- Consignee Address;
- Consignee Phone Number;
- Consignee Email Address;
- Marketplace Name;
- Buyer Account Number;[19]
- Buyer Address;
- Seller Phone Number;
- Buyer Phone Number;
- Marketplace Website;
- Buyer Name;
- Buyer Confirmation Number;
- Buyer Email Address;
- Carrier Name;
- Known Carrier Customer;
- Merchandise/Product Weight;

[18] The Harmonized Tariff Schedule of the United States Annotated (HTSA) provides the applicable tariff rates and statistical categories for all merchandise imported into the United States; it is based on the international Harmonized System, the global system of nomenclature that is used to describe most world trade in goods.
[19] A Buyer Account Number is an internal number specific to a buyer and assigned by marketplaces.

- Merchandise/Product Quantity; and
- Listed Price on Marketplace.

CBP may use any combination of the above data elements to segment risk with respect to Section 321 shipments. For example, CBP may crosscheck pilot data including enhanced product description and listed marketplace price against what is actually listed on the manifest to highlight shipment anomalies prior to its arrival in the United States. Upon inspection, CBP may further use certain data, such as Product Picture or Link to Product Listing, to validate the contents of the package.

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

The source of information will be the pilot participants (marketplace, carrier, freight forward, broker, or other e-commerce stakeholder selected to participate in the pilot). The pilot participant providing the information to CBP will collect the data as they normally do using their existing data collection mechanisms. For example, online marketplaces may already collect data on the buyer and seller when products are purchased. They would continue to do so under the scope of this pilot, and transmit to CBP through an established point-to-point connection.

2.3 Discuss how accuracy of the data is ensured.

CBP may hold shipments for physical examination based in part on data submitted under the pilot. During physical examination, CBP may compare the data transmitted for a particular shipment to the shipment itself to verify that the data is accurate. If CBP determines that a participant has failed to exercise reasonable care in the execution of its participant obligations (i.e., submitting timely and accurate data), CBP reserves the right revoke that participant's involvement in the pilot, as outlined in the Federal Register notice.[20]

2.4 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Since the TFTEA expressly increased the "de minimis" exemption value from $200 to $800, many articles valued at $800 or less imported by one person on one day became eligible for duty- and tax-free entry under Section 321 and its implementing regulation, 19 C.F.R. § 10.151, and thus for entry with fewer data collection requirements. Collecting additional data for such shipments may be viewed as undermining the scope of TFTEA's impact on trade facilitation.

Mitigation: This risk is mitigated. The de miminis exemption authorizes certain imported articles to pass duty- and tax-free, but does not prohibit CBP from taking necessary action to ensure that the importation complies with the laws of the United States. TFTEA's change to the de

[20] 84 Fed Reg. 35405 (July 23, 2019).

minimis value caused a dramatic increase in the volume of shipments making use of de minimis entry procedures, leaving CBP with less information about a greater number of shipments and with fewer data elements to use to effectively identify and target high-risk shipments. By conducting the Section 321 Data Pilot, CBP is expanding the collection of information from shipments that qualify for the de minimis exception. However, the impact on trade facilitation is mitigated because CBP has broad authority to collect advance data and inspect all cargo crossing the border for compliance with the customs laws, including those related to health, safety, and other risks pursuant to various statutory authorities.[21]

Privacy Risk: Because information is collected from carriers, brokers, and freight forwarders, as well as non-traditional CBP partners such as online marketplaces, CBP may receive inaccurate Section 321 Data Pilot filing information about individual Buyers and Shippers.

Mitigation: While information about a Buyer or Shipper, including the contents of the shipment and identifying information, is not submitted directly to CBP from the Buyer or Shipper, this information is still generally very accurate. The Buyer or Shipper has an interest in submitting correct information to the carriers, brokers, freight forwarders, or online marketplaces to properly receive or send the correct items. Therefore, this risk is mitigated based on the high degree of confidence in data submitted directly to the pilot participants, who then submit the information directly to CBP. All transactions are electronic, further limiting the risk of inaccurate information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP will use the data transmitted under the pilot to help identify shipment anomalies, highlight information gaps, and uncover other discrepancies indicative of high-risk shipments. Receiving information through ATS allows CBP to conduct targeting and risk assessments within the system. This process increases security by employing a risk-based approach to improve shipment security through targeted screening.

Participants may electronically transmit the requested information through an existing point-to-point connection with CBP. Alternatively, participants may authorize a carrier or broker participating in the pilot who has an existing point-to-point connection with CBP to transmit the information on their behalf. CBP will respond to the data transmissions with a confirmation of receipt and will use the transmitted information to conduct risk assessments. Risk assessment for each shipment will be based on multiple transmissions, as each transmission can be from different parties providing different data elements at various stages in the supply chain. Messages will be maintained in the ATS.

[21] *See, e.g.,* 6 U.S.C. 211(c) and (g); 19 U.S.C. 482, 1431, 1461, 1499, 1589a, 1595a; *see also* 19 CFR 162.6.

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. Section 321 data is stored in ATS, which builds a risk-based assessment for cargo and conveyances based on criteria and rules developed by CBP. ATS cargo relies on rules-based targeting to build a score for the cargo or conveyance to subsequently identify cargo and/or conveyances of interest.

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

In rare cases, CBP will share information with DHS users in accordance with Section 6.0 of this PIA; however, no other DHS components will have assigned roles and responsibilities within the system for this pilot.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Information collected as part of Section 321 Data Pilot may be used for purposes beyond the scope of the pilot.

Mitigation: This risk is mitigated. The Section 321 Data Pilot will not affect any current requirements and CBP is not waiving any regulations for purposes of the pilot, including all the regulations pertaining to the provision of advance data cited above, such as the ACAS and ISF regulations. All existing Trade Act of 2002 requirements and all manifest requirements continue to apply. Additionally, CBP will not use the information transmitted pursuant to the pilot for entry or release purposes, and pilot participants cannot rely on information transmitted through the pilot for entry or release purposes.

Access to Section 321 data in ATS is role-based, and ATS user roles are highly restricted and audited. Access is restricted in the form of Mandatory Access Control, which is based on a demonstrated "need to know." Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP personnel with access to ATS are required to complete security and data privacy training on an annual basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

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.

CBP has provided notice to the public of the Section 321 Data Pilot through a Notice in the Federal Register on July 23, 2019 announcing the pilot.[22] In addition, this PIA provides general notice of CBP's collection and use of Section 321 data.

However, due to the low dollar threshold for transactions that are subject to Section 321 (under $800), it is highly unlikely that Buyers will be aware that their transactions will be submitted to CBP as a part of this pilot. Many, if not most, Buyers that are impacted by this pilot are individual consumers as opposed to corporate entities familiar with trade regulations.

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

Participants who provide their information to CBP to participate in this pilot do so voluntarily. However, U.S. law requires persons seeking to import goods and merchandise in the United States to provide certain information to allow CBP to determine whether the goods/merchandise may enter the United States.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individual Buyers are not given notice by the pilot participants that their information is shared with CBP.

Mitigation: This risk is partially mitigated. CBP has published a Federal Register Notice describing the pilot and is conducting this PIA to provide further public transparency. However, CBP must rely on participating carriers, brokers, freight forwarders, and online marketplaces to provide clear and explicit notice to individuals prior to sharing information with CBP for this pilot. It is possible that individuals may not realize they are purchasing merchandise from outside the United States; however, as noted above, U.S. law requires persons seeking to import goods and merchandise in the United States to provide certain information to allow CBP to determine whether the goods/merchandise may enter the United States.

[22] 84 Fed Reg. 35405 (July 23, 2019).

Section 5.0 Data Retention by the project

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

CBP has not yet developed a Records Retention Schedule for information collected as part of the Section 321 Data Pilot. CBP will retain these records consistent with requirements for Permanent Records until a NARA-approved Retention Schedule is in place.

If Section 321 information is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations, or cases (i.e., specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances) will remain accessible for the life of the law enforcement matter subject to relevant NARA-approved Records Retention Schedules to support that activity and other enforcement activities that may become related.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that without an approved retention schedule CBP will retain information beyond the operational necessity of the information.

Mitigation: This risk cannot be mitigated until a finalized records schedule is published. CBP is actively creating new records schedules for all Agency records, including information collected pursuant to the Section 321 Data Pilot. In the interim, CBP must adhere to a permanent records retention until a NARA-approved retention schedule is in place for the Section 321 Data Pilot. In the event that Section 321 information becomes associated with a law enforcement investigation, CBP will maintain that information for as long as is required for the life of the investigation, which may be permanent.

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 will be used.

Section 321 Data information will be shared on a "need to know" basis as warranted by a specific request or Memorandum of Understanding (MOU), particularly with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, where DHS believes the information would assist enforcement of civil or criminal laws. For targeting purposes, there are occasions in which certain data elements are shared outside of DHS to garner assistance in vetting and information gathering. At times, this is done in collaboration with intelligence community partners who may have additional information not available to CBP.

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

The external sharing outlined above is consistent with the purpose of CBP's original collection of the information. CBP collects information to perform a risk-based assessment of conveyances and cargo in order to enhance CBP's ability to identify potential violations of U.S. law, potential terrorist threats, and other threats to border security. This supports CBP's enforcement of numerous federal laws at the border, and is consistent with the broader CBP mission of safeguarding the nation while facilitating legitimate trade and travel.

6.3 Does the project place limitations on re-dissemination?

When sharing information pursuant to a memorandum of agreement, CBP requires that the recipient first request permission from CBP prior to sharing any information with a third party. External users of ATS who want to have access to Section 321 Data Pilot information must meet the terms and conditions of the arrangements permitting their access to ATS in order to obtain and maintain access. Generally, CBP requires that the external users employ the same or similar security and safeguarding precautions as employed by CBP and only use the data for legitimate purposes. For CBP, ATS has role-based security. Users from other government organizations must use the ATS interface to access the system where access is limited via a user profile/role. ATS user roles are highly restricted and audited. Application access is restricted in the form of role-based access, which is based on a demonstrated need to know. Users may not re-disseminate information without prior express written consent by CBP.

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

Information shared outside of the Department is tracked through the use of the DHS 191, Accounting of Disclosure Form, or an MOU. CBP and DHS users of ATS prepare a DHS 191 form each time they share PII from ATS outside of DHS. CBP and DHS share information from ATS pursuant to the terms of an arrangement for access to one or more of the modules of ATS, or in accordance with the language of a letter of authorization, which facilitates the sharing of a limited number of records from ATS in response to a request for assistance from another law enforcement agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CBP will share with carriers advanced e-commerce information that they would not normally receive in the standard business process, in potential violation of the Trade Secrets Act.

Mitigation: In the e-commerce environment and with the advent of new data elements, traditionally regulated parties, such as carriers, are unlikely to possess all of the information

relating to a shipment's supply chain. Specifically, the shipment originator, final destination, and package contents are often unknown. As part of the advance e-commerce data that CBP receives pursuant to this pilot, some of the information will be impermissible to share with the carriers without violating the Trade Secrets Act. For the purposes of this pilot, this risk is mitigated since CBP will not share any information with carriers or online marketplaces.

Privacy Risk: There is risk that CBP will inappropriately share advance e-commerce data under inappropriate circumstances, or with individuals without a demonstrated need to know.

Mitigation: Risks related to sharing of information outside DHS, including any potential risk of further dissemination of information by the external agency to a third agency, are mitigated through arrangements governing access to Section 321 information in ATS by external parties and sharing of ATS information with external parties. Each arrangement defines the nature of the outside access to or sharing of ATS information, including the scope of the ATS information being accessed or shared and the legal basis upon which they receive it. The arrangements generally require the external party accessing or receiving information to employ measures relating to security, privacy, and safeguarding of information that are equivalent or comparable to measures employed by DHS. As a general matter, the arrangements also stipulate that any further dissemination of ATS information by the receiving party to a third party is subject to prior authorization by CBP. Lastly, CBP emphasizes that within each arrangement, each external user is provided with training designed to ensure that data accessed through ATS is safeguarded and secured in an appropriate manner and that dissemination restrictions are observed, consistent with applicable laws and policies.

Section 7.0 Redress

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

Individuals seeking access to Section 321 information may file a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection
Freedom of Information Act Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-1476

All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible on subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of

information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

Because of the law enforcement nature of information in ATS related to the risk assessment of any Section 321 information, DHS has exempted portions of this system from the notification, access, amendment, and certain accounting provisions of the Privacy Act of 1974. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records with appropriate exemption in place. To the extent that a record is exempted in a source system, the exemption will continue to apply.

Notwithstanding the applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would 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 procedures and points of contact published in the applicable SORN.

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

Inquiries and efforts to request correction of CBP records may be directed to:

U.S. Customs and Border Protection
CBP Info Center
Office of Public Affairs
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

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

This PIA and the applicable SORNs provide general notice regarding the procedures for accessing, correcting, or amending Section 321 information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Section 321 participants may be adversely impacted by the CBP cargo screening process based on a few select data elements.

Mitigation: CBP has designed the Section 321 filing process to ensure that the importation and entry process is secure and seamless for the participant. Filers who do believe that they have

been adversely impacted may seek redress as described in this PIA and the applicable SORNs. CBP seeks to permit all persons to be able to obtain copies of the Section 321 data that the relevant participant submitted to CBP pursuant to regulatory requirements. As noted above in paragraph 7.1, individuals may also seek access to such information submitted to CBP pursuant to the FOIA, and as a matter of CBP policy redress may also be requested.

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?

Section 321 information is only available to specific users within the Office of Field Operations and Office of Trade via ATS, which has role-based access. All user groups have access to the system as defined by their specific profile. Access is restricted based on roles and a demonstrated need to know.

Pilot data is specifically marked by a label and section headings within the ATS Import Cargo shipment details page and user interface. This data will have its own specific user role, which will need to be provisioned to users based on business sponsor approval. Only CBP officials with the specific Section 321 Data Pilot role will have the ability to view the data in the ATS Import Cargo application.

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

Initial ATS access is not activated for any user without completion of the CBP Security and Privacy Awareness course. The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and ATS users are required to take the course 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?

Each user groups' access to information in ATS is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common rights and mission responsibilities of users within the group. Access by Users, Managers, System Administrators, Developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions. User access to data is based on a

demonstrated need-to-know by a user, and access is only granted with supervisory approval and upon completion of the required security checks.

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?

Any access agreements that are put into place for the Section 321 data will be drafted by the business owners with input from the program managers. Each agreement will define the nature of access to ATS for the Section 321 Data Pilot, including specific modules and scope of information subject to the sharing agreement. All information arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

Responsible Officials

Laurie Dempsey
Director
Intellectual Property Rights (IPR) Policy and Programs Division
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

[Original, signed copy complete and on file with the DHS Privacy Office]

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security