Privacy Impact Assessment
for the

e-Allegations Portal

DHS/CBP/PIA-060

October 22, 2019

Contact Point
Deborah Augustin
Trade Remedy Law Enforcement Division
Office of Trade
U.S. Customs and Border Protection
(202) 325-6727

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for securing the United States and its borders while facilitating lawful travel and trade. The CBP Office of Trade (OT) facilitates lawful international trade activities, enforces violations of various trade laws and regulations, and investigates allegations of trade violations made by the members of the public. CBP created a public-facing website called "e-Allegations" for members of the public and the trade community to report potential violation of criminal and trade laws and regulations. CBP is conducting this Privacy Impact Assessment (PIA) to assess the privacy risks associated with the collection, use, and dissemination of personally identifiable information (PII) submitted via e-Allegations.

Overview

CBP has a dual mission of protecting national security objectives while facilitating legitimate trade and travel, and plays a vital role in promoting the country's economic prosperity and security. CBP collects the second largest amount of revenue of any agency in the Federal Government and CBP operations have a significant impact on the security and facilitation of legitimate international commerce and America's economic competitiveness.

In the performance of its trade enforcement operations, CBP has identified several high-risk areas designated as Priority Trade Issues (PTI) that can cause significant revenue loss, harm the U.S. economy, or threaten the health and safety of the American people. PTIs drive risk-informed investment of CBP resources and enforcement and facilitation efforts, including the selection of audit candidates, special enforcement operations, outreach, and regulatory initiatives. The five current PTIs are Intellectual Property Rights; Textiles and Apparel; Import Safety; Trade Agreements; and Antidumping and Countervailing Duties (AD/CVD).

Under the Tariff Act of 1930,[1] as amended (Tariff Act), U.S. industries may petition the Government for relief from imports that are sold in the United States at less than fair value ("dumped") or that benefit from subsidies provided through foreign government programs. Under the law, the U.S. Department of Commerce determines whether the dumping or subsidizing exists and, if so, the margin of dumping or amount of the subsidy. The United States International Trade Commission determines whether there is material injury or threat of material injury to the domestic industry by reason of the dumped or subsidized imports. AD/CVD has been identified by CBP as a PTI because collection of these duties is critical to the U.S. economy and U.S. business competitiveness.

[1] 19 U.S.C. Chapter 4.

While the vast majority of manufacturers, importers, customs brokers, and other parties involved in shipments of goods subject to AD/CVD orders accurately provide their shipment information to CBP and lawfully pay the duties due, CBP has a core statutory responsibility to collect all revenue owed to the U.S. Government that arises from the importation of goods. CBP's AD/CVD trade program works to ensure that CBP implements a concerted, systematic approach to detecting and deterring the circumvention of AD/CVD laws, and liquidating transactions in a timely and accurate manner, while facilitating legitimate trade.

Pursuant to the Tariff Act, CBP is authorized to assess and collect duties, taxes, and fees incident to international traffic and trade. CBP also provides procedural guidance to the trade community[2] to enhance and increase compliance with domestic and international customs laws and regulations. By ensuring compliance with various customs laws and regulations, CBP helps importers ensure that their shipments are free from terrorist or other malicious interference, tampering, or corruption of containers or commodities, including human rights violations involving forced labor.[3] As described by Congress in the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA),[4] CBP also has the responsibility to protect national economic security, facilitate fair trade, support the health and safety of all people, ensure a level playing field for U.S. industry, and prevent evasion of duties imposed by antidumping and countervailing orders.

e-Allegations Portal to Report Trade Allegations

CBP is committed to protecting national economic security and enforcing U.S. trade laws and regulations, including to combat trade fraud. CBP accomplishes this mission by detecting high-risk activity, deterring non-compliance, and disrupting fraudulent behavior. To do so, CBP uses all methods at its disposal, including increased bonding, enhanced targeting and inspection of high-risk imports, and reviewing allegations of non-compliance to ensure a fair and competitive trade environment.

Created in 2008, the e-Allegations[5] online portal on the CBP.gov website has served as the main portal for receiving allegations of commercial trade violations and other illegal activity affecting the U.S. commerce. The portal contains a U.S. Immigration and Customs Enforcement (ICE)/Homeland Security Investigations (HSI) link for allegations specific to immigration,

[2] A member of the "Trade Community" is an entity that has standing as a manufacturer or trading partner in one of the 10 sectors (e.g., automotive/aerospace, pharma/health/chem.).
[3] CBP regulations state that any person who has reason to believe that merchandise produced by forced labor is being, or is likely to be, imported into the United States may communicate his belief to any Port Director or the Commissioner of CBP (19 C.F.R. § 12.42).
[4] TFTEA was signed into law as Public Law 114-125 on February 24, 2016. It is the first comprehensive authorization of CBP since the Department of Homeland Security was created in 2003, with the overall objective to ensure a fair and competitive trade environment.
[5] The e-Allegations website is CBP's online violation reporting system portal, located at: https://eallegations.cbp.gov/Home/Index2.

narcotics, and other non-trade criminal violations, facilitating the efficient referral of non-trade issues to ICE for processing.[6] CBP does not investigate or maintain information regarding non-trade issues that are referred to ICE.

CBP maintains allegations of trade-related violations that may involve: misclassification of merchandise; country of origin markings; health and safety violations; agriculture violations; intellectual property rights violations; and textile or other trade violations. e-Allegations expanded in 2016 to include a separate portal for allegations about violations of the Enforce and Protect Act (EAPA) of 2015.[7] The EAPA allegations section of the e-Allegations portal facilitates the enforcement of antidumping and/or countervailing duties (AD/CVD) evasion schemes against U.S. importers. The public may submit anonymous allegations for evasion of AD/CVD against U.S. importers via the e-Allegations Portal, but all EAPA allegations require basic contact information about the submitter. CBP still receives informal allegations via mail, telephone, and email correspondence, but now tracks them via e-Allegations.

Types of Trade Allegations

The e-Allegations web site provides public users with three options for reporting the different types of allegations over which DHS has authority:

Trade Violations

Members of the public may use the "Report Trade Violations" link to report suspected illegal trade activity by trade related entities such as importers, exporters, brokers, consignees, trade filers, or other trade related business entities. Suspected violations include:

- Intellectual property rights infringements;
- Textile or free trade agreement violations;
- Health and safety issues;
- Classification and value violations;

[6] Individuals are redirected to the ICE HSI Tip Form: https://www.ice.gov/webform/hsi-tip-form. This PIA, and all other privacy compliance documentation associated with the allegations of individuals for investigations pursuant to ICE's law enforcement and investigative authorities and mission, is under the purview of ICE. Although the public can access HSI Tip Form via a link on the CBP's e-Allegations cloud-based website, the allegations submitted through the CBP's e-Allegations for ICE TIPS are managed separately from CBP e-Allegations. The information collected by ICE TIPS is outside the scope of this PIA. More information about ICE and Reporting Suspected Criminal/Illegal Activity can be found in the FALCON Tipline PIA at: https://www.dhs.gov/sites/default/files/publications/ice-pia-033-falcon-tipline-2012.pdf.

[7] Title IV of TFTEA, Prevention of Evasion of Antidumping and Countervailing Orders (cited as EAPA), tasks CBP with investigating and preventing evasion of duties imposed by antidumping and countervailing orders.

- Forced labor violations; and
- Non-EAPA allegations.

Individuals may use the fillable electronic form to submit an allegation anonymously or may provide their name and contact information if they chose to do so. The submitter may provide information about the type and description of the violation, country of export, product (Harmonized Tariff Schedule (HTS) code, if known), and suspected violator (importer/exporter name/company name).[8]

Evasion Violations via EAPA

EAPA establishes the procedures for submitting AD/CVD allegations of evasion against importers to ensure fair trade practices and ensure a level playing field for U.S. industry. The online EAPA Allegations submission form is restricted to trade allegations made by members of the trade community (trade-related entities such as importers, exporters, brokers, consignees, trade filers, or other trade related business entities) who have a vested interest, or "standing," in relation to AD/CVD orders. Accordingly, they must identify themselves when submitting an allegation.

Members of the trade community who meet the definition of an interested party as defined by statute must:

- Provide a statutory description of covered merchandise and applicable AD/CVD order(s) pertaining to their allegation; and
- Demonstrate that evasion of an AD/CVD order has occurred.[9]

As provided for under 19 CFR § 165.16, CBP shares in-scope referrals to the U.S. Department of Commerce (DOC) if CBP cannot determine whether the type of import/merchandise described in an allegation is properly within the scope of an AD/CVD order. The referral may contain any information necessarily relevant to the AD/CVD order/case to allow DOC to examine and determine if commodities fall within or without of the AD/CVD duty orders.

Internal Management of Allegations

CBP uses the Commercial Allegation Recording System (CARS), a web-based SharePoint portal, to receive, record, review, manage, and track all trade allegations. CBP trade analysts use CARS to view and reference allegations on importers (and in some cases, exporters) and/or commodities as they encounter imports arriving at the ports of entry. CARS also provides administrative and reference information such as port codes, trade laws, and information about

[8] This information is used to identify the alleged violator providing the violator is a business, or individual "doing business as" who has registered as, or is importing merchandise as an importer, broker, consignee, etc.
[9] At the time of publication of this PIA, the only such EAPA allegation that is permissible through this link is that with a nexus to AD/CVD. If and when the link for reporting EAPA violations is expanded to include other trade-related violations, an update with be made to the corresponding CARS privacy threshold analysis (PTA).

Field Offices. CARS also includes an online CARS User Manual to ensure that all users have a full understanding of their roles and responsibilities.

CARS contains the allegation case number, company/importer/exporter/broker name, email/physical address, phone, and number. The source of an allegation can use and include any information known to them or suspected about violators in their submission, such as an Importer ID or Social Security number (SSN).[10] All information provided is retained in CARS/EAPA without bias, to maintain the integrity of the allegation submitted.

AD/CVD allegations in EAPA are different from standard e-Allegations in CARS only insofar as EAPA entries of alleged violations can only be made by members of the trade community, whereas e-Allegations entries can be made by anyone. If a determination needs to be made based on an allegation of whether an import item/merchandise falls within an AD/CVD order, CBP does not perform the research into the import item/merchandise; rather, it is the responsibility of DOC, under 19 CFR § 165.16. Such referrals to DOC are made as part of the investigation process and performed on an ad-hoc basis by the CBP EAPA Investigations Branch.

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?

DHS's law enforcement jurisdiction is highly complex and derives authority for U.S. trade related activities from a wide spectrum of federal statutes. CBP and ICE enforce customs laws related to Title 19 U.S. Code and regulations in Title 19 of the Code of Federal Regulations in support of tariff and revenue protection pursuant to The Tariff Act of 1930, as amended, and other laws and regulations.

These include 19 CFR parts 19, 101, 111, 112, 113, 141, 142, 148, and 163; 19 CFR §§ 24.5, 103.31(e), 192.14, and 149.3; 31 CFR Chapter X; Public Law 109-347, 120 Stat. 1884 (Oct. 13, 2006); 5 U.S.C. § 301; 6 U.S.C. § 202; 8 U.S.C. §§ 1103; 1357, and 1360; 19 U.S.C. §§ 66, 1431, 1448, 1481, 1484, 1505, 1514, 1624, and 2071; note: 26 U.S.C. § 6109(d); 31 U.S.C. § 7701(c); Title 18, U.S.C.; 19 U.S.C. §§ 66, 482, 1431, 1448, 1467, 1481, 1484, 1485, 1498, 1499, 1505, 1509, 1514, 1551, 1551a, 1555, 1565, 1581(a), 1589a, 1624, 1641, and 2071; 44 U.S.C. Chapter 31 (Federal Records Act), § 3101; 31 U.S.C. 7701(c); § 203 of the Security and

[10] If an importer does not have an Importer ID, the importer can use his/her SSN, or other tax information in lieu of an Importer ID on trade related forms for the importation of goods; likewise, an individual making the allegation can include whatever text (such as Importer ID, Taxpayer Identification Number, SSN) that is known to him/her in the e-Allegations system form, thus an Importer ID or SSN can be entered into CARS.

Accountability for Every (SAFE) Port Act of 2006 and § 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002.

CBP also has the authority to share information with the U.S. Department of Commerce pursuant to 19 CFR § 165.16. In more detail, and as applicable, the Import Information System SORN includes a complete list of authorities pursuant to the U.S. export laws CBP is responsible for enforcing.

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

SORN coverage for information submitted to CBP as part of a trade allegation are covered by the DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS) SORN.[11] Records maintained pursuant to the SEACATS SORN are used to (1) document individuals and businesses who violated, or are alleged to have violated, Customs, immigration, agriculture, and other laws and regulations enforced or administered by CBP; (2) collect and maintain records on fines, penalties, and forfeitures; and (3) collect and maintain records of individuals who have provided assistance with respect to identifying or locating individuals who have or are alleged to have violated Customs, immigration, agriculture, and other laws and regulations enforced or administered by CBP. SEACATS specifically permits the collection of information about current and former violators and alleged or otherwise suspected violators of Customs, immigration, agriculture, or other laws and regulations administered or enforced by CBP, and related parties involved in, or affected by, an inquiry concerning the violation of Customs, immigration, agriculture, or other law enforced or administered by CBP.

As part of the investigatory or analysis process of the trade allegations, CBP may take a trade enforcement action, generate trade intelligence records, or both. Trade enforcement actions are covered by the SEACATS SORN as noted above, and also by the CBP TECS SORN,[12] which covers trade records related to a violation or suspected violation of law that CBP enforces or administers. TECS tracks individuals who have violated or are suspected of violating a law or regulation that is enforced or administered by CBP, provides a record of any inspections conducted at the border by CBP, determines admissibility into the United States, and records information regarding individuals, firms, and organizations to whom CBP has issued detentions and warnings.

In the event that information submitted as part of an e-Allegation is used to generate a Trade Threat Analysis or other kind of trade intelligence product or alert, these records are covered by the CBP Intelligence Records System SORN,[13] which covers law enforcement, intelligence,

[11] DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008 73 FR 77764.
[12] DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008 73 FR 77778.
[13] DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198.

crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by CBP.

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

Yes. A system security plan has been completed for both the CBP.gov portal and the backend application, consistent with requirements of the Federal Information Security Modernization Act of 2014. Both ATOs are valid through Spring 2021.

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

No. CBP Records Management is in the process of establishing a records retention schedule for the CBP systems in which the CBP website and CBP SharePoint sites are maintained. CBP Records Management will work with the respective program offices to establish the appropriate schedules with NARA.

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

CBP collects data directly from members of the public, and therefore is subject to the Paperwork Reduction Act (PRA). The Office of Management and Budget (OMB) Control Number 1651-0131 applies to CBP collections of information related to trade allegations ("e-Allegations").

Section 2.0 Characterization of the Information

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

Through the e-Allegations web portal, CBP collects information pertinent to the alleged violation, including (1) information about the individual making the allegation, as required; (2) information about the alleged violator; and (3) information about the suspected violation, including suspected violation type, AD/CVD duty order number, or information about merchandise. Once information is provided to CBP through the e-Allegations portal the information is transferred via a secure web service to CBP's Commercial Allegation Recording System (CARS) SharePoint site[14] for further review, processing, or adjudication. The CBP CARS SharePoint site is accessible

[14] Within CARS, a unique case number is assigned.

by CBP employees enabling them to track commercial allegations, enforcement actions, and prior disclosures.

The e-Allegation information intake page also contains an attachment option where a submitter is permitted to upload up to five document files[15] to his/her allegation. The submitter must indicate which type of allegation he/she are submitting in order for a system-generated reference number to link the attachments to the correct allegation. The attachments provided by the submitter can be attached to the information provided and added to CARS.

CBP collects the following information from individuals using the web portal for reporting *Trade Violations*:

- Information about the individual making the allegation:
  - First, Middle, and Last name;
  - Email address;
  - Phone number; and
  - Role (broker, carrier/freight forwarder, consumer, domestic manufacturer, exporter, foreign manufacturer, government, importer/competitor, lawyer, or other).
- Information about the Allegation
  - Violation Type: Classification of Merchandise, Country of Origin Markings, Description of Merchandise, Forced Labor, FTA/Preference Claim, Health and Safety, Intellectual Property Rights, Jones Act Violation, Prohibited Items, AD/CVD, Smuggling, Textiles, Valuation, or Other;
  - Violation description (using a free flow text box);
  - Country of Export; and
  - Product Category (identified by using the dropdown menu of Harmonized Tariff Schedule of the United States (HTSUS) codes 01-97, including option for unknown/multiple).
- Information about the alleged violator:
  - Violator name;
  - Address, city, state, province or U.S. possession, Zip Code, Country; and

[15] Attachment file types must be in .jpg, .gif, .pdf, .doc, .docx, or .txt format. Each file is limited to 2MB. Files exceeding the 2MB limit or other hard copy materials can be submitted via mail to the address listed on the FAQ page for e-Allegations: https://www.cbp.gov/trade/trade-community/e-allegations/e-allegations-faqs.

- Information about any additional parties (using free flow text box).

CBP collects the following information about individuals reporting *Evasion Violations via the Enforce and Protect Act (EAPA)*:

- Information about the individual making the allegation:
  - Private Sector Entity/U.S. Government Entity/Small Business name;
  - First, Middle, and Last name;
  - Email address and phone number; and
  - Business or company name, mailing or business address, email address, (and if acting on behalf of another company, their information).
- Information about the allegation:
  - AD/CVD Order Number;
  - Product description (using a free flow text box);
  - HTSUS product category; and
  - Evasion violation description (using a free flow text box).
- Information about the alleged violator:
  - Name of importer suspected of evasion; and
  - Violator address, city, state, country, Zip code.
- Certification and informed consent:
  - Certification by the submitter related to the allegation pursuant to 19 CFR §§ 165.4(a) and (d), 165.5(b)(2), 165.7(a); and
  - Acknowledgement of informed consent pursuant to 19 CFR §§ 165.11(b)(1) through (5), and (c).

Information submitted to CBP through other means (e.g., standard or email) may contain additional information at the submitter's discretion since these mechanisms do not provide a standard format for collection.

In addition to the information provided by the submitter, CBP may maintain other relevant information pertinent to the investigation, including information from other CBP trade and law enforcement systems within CARS.

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

CBP receives this information from the public, including from individuals, members of the trade community, and from federal, state, and local, tribal, territorial, or international agencies with the responsibility for oversight of trade/merchandise for import/export to/from the United States. Information can be submitted to CBP via the e-Allegations website, by mail, or by email.

CARS also includes information obtained from internal CBP transactional systems such as the Automated Commercial Environment (ACE).[16]

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

By its nature as a trade information system, information sent to CARS from the e-Allegations portal necessarily will include commercial information since the allegations involve some kind of commercial entity. However, all information is submitted by the individual or entity filing the allegation. As part of the investigatory process, CBP trade analysts may use commercial and open source information to adjudicate the allegation.

2.4 Discuss how accuracy of the data is ensured.

Information sent to CARS from the e-Allegations portal is not altered in any way, due to the need to maintain the integrity of the information as it was received by the submitter. During the investigative or analysis processes, CBP may make a determination that information received via e-Allegations is false or inaccurate, and the results of the investigation and analysis will be retained in CARS in the final determination results.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information submitted from the public via e-Allegations to CBP may be incorrect, or that someone could submit misinformation about another member of the Trade Community to CBP.

Mitigation: This risk is inherent to any Government collection of tips, leads, or allegations. Due to the potentially inaccurate nature of allegations, CBP does not use e-Allegations as a means

[16] For information about trade processing generally, *see* DHS/CBP/PIA-003 Automated Commercial Environment (ACE), *available at* https://www.dhs.gov/publication/filing-data-acsace. ACE is the backbone of CBP's trade information processing and risk management activities and is the key to implementing many of the agency's trade transformation initiatives. ACE allows efficient facilitation of imports and exports and serves as the primary system used by U.S. Government agencies to process cargo.

to ascertain whether the allegation is accurate as entered, but rather, it is intended to provide the public with a means to share with CBP as much information as they have based on their own observations of the alleged criminal/illegal activity. Information sent to CARS from e-Allegations is not edited, corrected, or altered in any way, so as to maintain the integrity of the information as it was received by the submitter. If during the investigative or analysis process, CBP makes the determination that information received via e-Allegations is false or inaccurate, the final results of the investigation and analysis will be retained in CARS, and the necessary actions against the alleged individual or business, if warranted, will be reflective of the results of the thorough investigation, and not the allegations.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP collects PII from members of the public primarily via the e-Allegations web portal, however, the same information can be sent to CBP by mail to:

Office of International Trade
U.S. Customs and Border Protection
1300 Pennsylvania Ave., NW, ATTN: 1400 L-11
Washington, D.C. 20229
Or by e-Mail to CBP at: eapallegations@cbp.dhs.gov.

This information can be from and about anyone involved in the importation and exportation of merchandise and international trade. Using e-Allegations, CBP collects PII for two purposes: 1) to permit individuals making allegations about criminal activity[17] or violations of trade laws to identify those who they suspect of making the violation; and 2) to allow individuals to identify themselves as the alleger (in some instances this is optional, however, in others, it may be mandatory, for example in the case where an email is submitted and the submitter's email is retained from the email, or when the submitter requires a confirmation receipt or reference number from his/her allegation).

CBP uses information received from the public to identify potential violators and search existing CBP trade records in order to open and carry out an investigation. Investigations include but are not limited to research into importer and exporter histories, open source research, analysis, site visits, cargo inspections, entry reviews, interviews, regulatory audits, and obtaining additional information from allegers and alleged violators and/or their legal counsels. The results of the investigations may result in trade enforcement actions such as duty demands, penalties, interim

[17] The public is instructed to report criminal or suspicious activity of immediate concern, including terrorism-related or other imminent threats to public health and safety, to ICE at: 1-866-DHS-2-ICE (1-866-347-2423).

measures, seizures of merchandise, and the creation of trade enforcement records; or may result in the creation of trade intelligence products such as trade threat analyses.

Contact information about the submitter (name, email address) is optional in most cases, but may allow CBP to follow up with the submitter or allow the submitter to submit images and receive a confirmation number for the allegation. Within CARS, CBP also maintains general contact information for the CBP employee/supervisor supporting the import activity, allegation, or investigation.

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. Neither e-Allegations portal, nor the CARS Sharepoint site, use technologies to discover predictive patterns or anomalies.

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

No. The e-Allegations portal serves as pointer to the ICE website through the "Report Suspected Criminal/Illegal Activity" tab for the public to report potential criminal activities, but CBP does not store any information associated with this referral. No other DHS components have access to CARS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP will use the information in the system for purposes beyond what is described in this PIA.

Mitigation: CARS includes an online CARS User Manual to ensure those accessing CARS have a full understanding of their roles and responsibilities. By providing access to all employees, CARS allows CBP trade analysts across the country to view and reference allegations on importers (and in some cases, exporters), and/or HTSUS codes related to the commodities that they encounter upon inspection of imports arriving at the ports of entry. Although all CBP employees are able to access CARS using a secure link, not all employees will have the ability to make changes to the allegation information contained therein. However, there remain some unmitigated risks associated with the fact that CBP employees without a need to know have view-only access to trade allegation information.

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.

All trade-related business entities are responsible for understanding and complying with U.S. trade law and regulations, including 19 U.S.C. §§ 4372 and 4318; Title IV, § 421 of TFTEA; and importing laws and regulations about the import process for importing merchandise into the United States. CBP provides guidance for "Importing Into the United States" on its website,[18] including information in Chapter 39 on "Special Requirements" that provides information on items that may require licenses or permits, such as food products, plants, animals, dairy, prescription medications, trademarked articles such as name-brand shoes, handbags, luggage, golf clubs, toys, and copyrighted material such as CDs, DVDs and tapes.

CBP provides extensive notice to the public through its public facing website, which discusses where to submit inquiries about an allegation, what is needed to submit an allegation, and includes a link to frequently asked questions. CBP also explains when a submitter may remain anonymous and when the submitter's identity is required. More information about who may submit an EAPA allegation (i.e., what defines an interested party with standing) and the authorities surrounding this type of allegation can be found on the third link of the e-Allegations website.[19] Small businesses requesting assistance in reporting an AD/CVD allegation for EAPA violations can contact eapallegations@cbp.dhs.gov.

Due to the nature of the allegations, CBP cannot provide timely notice to individuals about whom an allegation is submitted. Doing so might compromise CBP's ability to investigate the claims. In part due to this lack of direct notice, CBP is publishing this PIA to notify members of the public of CBP's collection of trade allegations information through this program.

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

The submission of an allegation to CBP is voluntary. While CBP can collect information about the submitter, submitters may also choose to remain anonymous by not providing information about themselves. However, CBP cannot investigate EAPA claims that are submitted anonymously, and other anonymous claims may hamper CBP's enforcement efforts when further contact with the submitter may be helpful to obtain more detailed information. CBP endeavors to protect any information provided by a submitter from public disclosure.

[18] https://help.cbp.gov/app/answers/detail/a_id/197/noIntercept/1.
[19] https://eallegations.cbp.gov/Home/Index2#.

In most cases, the Privacy Act, the Trade Secrets Act, and CBP regulations prevent CBP from disclosing information about the submitter. Additionally, because of the Trade Secrets Act, information about the member of the trade community who is the subject of the allegation, including results of any research conducted or outcomes of an investigation, can also be withheld from disclosure.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that members of the trade community may not be aware that someone has submitted to CBP an allegation of trade violations pertaining to them.

Mitigation: This risk is partially mitigated. CBP provides information on its website for international trade requirements, and information related to the submission of online trade violations. In addition, CBP is publishing this PIA to further explain that trade allegations may be submitted against any entity that violates U.S. Trade Law. However, due to the nature of the allegations, CBP cannot provide timely notice to individuals about whom an allegation has been submitted.

Section 5.0 Data Retention by the project

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

Information collected via the e-Allegations Portal has no specific, NARA-approved, retention schedule. However, CBP currently has a new Agency-specific retention schedule in draft that proposes that trade allegations records be "cut off at close of case or completion of litigation and all appeals, whichever is appropriate," and destroy the records ten years after cutoff.

In the interim, CBP will retain the records in accordance with the published SEACATS SORN. Records related to a law enforcement action, or that are linked to an alleged violation of law or regulation, or are matches or suspected matches to enforcement activities, investigations, or cases (i.e., administrative penalty actions or criminal prosecutions), will remain accessible until the conclusion of the law enforcement matter and any other enforcement matters or related investigative, administrative, or judicial action to which it becomes associated plus five years. Records associated with a law enforcement matter, where all applicable statutes of limitation have expired prior to the conclusion of the matter, will be retained for two years following the expiration of the applicable statute of limitations.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CBP will retain allegations information in the CARS SharePoint collaboration site for longer than necessary to conduct an investigation into trade violations.

Mitigation: This risk is partially mitigated. Information collected via the e-Allegations Portal has no specific, NARA-approved, retention schedule. However, CBP is actively working to create and publish an Agency-specific records schedule for e-Allegations. In the interim, CBP will retain the records in accordance with the published SEACATS SORN.

Section 6.0 Information Sharing

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

CBP is obligated by law to share in-scope referrals to the U.S. Department of Commerce (DOC) or the United States International Trade Commission (USTC) under 19 CFR § 165.16 if, at any point after receipt of an allegation, CBP cannot determine whether the merchandise described in an allegation is properly within the scope of an AD/CVD order. The referral may contain any necessary information made available to CBP regarding whether the merchandise described in an e-Allegation submission is subject to the relevant AD/CVD orders. CBP will then place the determination by the DOC on the administrative record of CBP's proceeding and will electronically notify the parties to the investigation providing that doing so does not violate the Trade Secrets Act.

In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the SEACATS SORN and as otherwise authorized under the Privacy Act. In addition, CBP may share trade related information with appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing trade laws.

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

Routine Use G allows DHS to share trade related information to appropriate federal, state, local, tribal, or 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, license, or treaty when DHS determines that the information would assist in the enforcement of civil or criminal laws. This sharing relates to the enforcement of trade-related laws, consistent with the purpose for which CBP collects the information.

6.3 Does the project place limitations on re-dissemination?

Yes, CBP limits onward sharing by requiring that recipients of the information specify to CBP any parties with which they intend to share, or have statutory obligations to share, CBP trade-related information.

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

To obtain trade data from CBP related to e-Allegations, or any other trade system, the requesting party must submit a written request for specific information as noted in Section 7, and state how it plans to use the information in relation to importing commercial goods into the United States or its nexus to a law enforcement matter. CBP retains a copy of this request and submits it to the CBP Privacy Office for review. Once the CBP Privacy Office reviews the request, based on the circumstances of each case, a CBP Privacy official drafts an authorization memorandum specific to each case. CBP retains a copy of the memorandum. If the disclosure is approved, CBP also maintains a record of the disclosure using DHS Form 191.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that further external sharing may occur, or could include more information than necessary, and will not be properly recorded as required by the Privacy Act.

Mitigation: Through a formal disclosure authorization process CBP provides notice to the releasing authority within CBP (CBP data owners) of their obligations to only pull what data is relevant to the request, to redact any identifiable names, PII or sensitive PII of DHS personnel, and any computer screen codes and internal file codes. CBP also advises the data recipient that information is provided only for the purpose stated in their request and may not be employed for any other use. Further sharing is also restricted in so far as the data must not be released to another agency or any other third party without CBP's express written consent. In the event of any unauthorized release on its part, the requesting office will intercede on CBP's behalf to assume responsibility for all expenses, costs, or liabilities arising from such disclosure.

Section 7.0 Redress

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

Individuals seeking access to certain CBP records may file a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, or mail a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) 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 the 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

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

If an individual believes CBP records related to trade allegations or other activities may be inaccurate, inquiries may be directed to the CBP Privacy Officer as described above or at privacy.CBP@cbp.dhs.gov.

Information sent to CARS from e-Allegations is not edited, corrected, or altered in any way, so as to maintain the integrity of the information as it was received from the submitter. If during the investigative or analysis process CBP makes the determination that information received via e-Allegations is false or inaccurate, the final results of the investigation and analysis will be retained in CARS, and the necessary actions against the alleged individual or business, if warranted, will be reflective of the results of the thorough investigation, and not the allegations. If at that time, the subject of the investigation disagrees with the findings, he or she may submit or make permissible amendments or corrections to their records or statements.

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

In general, this PIA and the CBP website provide notice to individuals related to procedures for correcting information maintained by CBP. CBP also provides general contact information on the e-Allegations Portal for general inquiries. Individuals may correct previously submitted allegations by contacting the EAPA mailbox at eapallegations@cbp.dhs.gov. However, as a result of an allegation being made by members of the general public, or the trade community, businesses (e.g., importers, brokers), individuals alleged of any trade violation may be unaware of their information being included in an allegation at all, unless they are made aware by being involved in an active investigation.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will have a limited opportunity to access and correct their data in the system or may not know that they have the ability to access/correct the information.

Mitigation: This risk is partially mitigated. Redress for trade activities is managed and outlined in the ACE PIA; however, allegations of potential trade violations may be exempt from certain provisions of the Privacy Act. Permitting access to the records contained as part of a CBP trade allegation could inform violators of CBP's law enforcement techniques or activities. Access to these records could also permit the violator to impede CBP's investigation, to tamper with witnesses or evidence, and to avoid detection, seizure, or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on law enforcement agencies. The existing redress procedures are adequate to address the individual's right to access and correct his or her records and comply with all legal and policy requirements.

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?

CBP must ensure that all allegations are maintained in CARS in their original form and are available and accurate as originally presented in the e-Allegation system to ensure a proper and thorough investigation. Therefore, allegations uploaded to the e-Allegations portal are managed through the Office of Trade standard operating procedures. The CARS staff will provide notice to the Chief of a CARS allegation when filed. All documents uploaded are monitored by CARS paralegal staff and managed by the CARS staff, who are responsible for specific cases identified for additional review/audit.

In addition, the CBP Office of Trade secures information by complying with the requirements of the DHS Information Technology Security Program Policy. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules. In order to gain access to Office of Trade systems and information (including office-specific SharePoint portal sites), a user must not only have a need-to-know, but must also have successfully undergone a single-scope background investigation and completed annual privacy training. A supervisor submits the request to the CBP Office of Information and Technology (OIT) indicating the individual has a need-to-know for official purposes depending on the user's role within the system. CBP OIT verifies that the

necessary background check and privacy training have been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Further, CBP and Office of Trade systems have audit logs to track the use of the system and as well as conducting periodic reviews for abuse.

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

Initial access to CBP systems and information is not activated for an individual 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 all CBP employees are required to take the course annually.

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

All employees with access to the CBP network may view the CARS SharePoint site only after: 1) passing a single-scope background investigation, 2) completing annual privacy recertification courses, 3) being assigned a user profile for the home port area in which they are stationed, and 4) being assigned duties that give them an official need to access the system. All background investigation and training records associated with users who have access to CBP and Office of Trade systems are kept in Cornerstone,[20] and routine audits are performed to ensure individuals are not accessing the information without a need-to-know, which is established when access is granted to the respective systems for which they must operate, by requiring supervisor approval.

[20] *See* DHS/CBP/PIA-038 Cornerstone (February 27, 2017), available at https://www.dhs.gov/publication/dhscbppia-038-cornerstone.

8.3 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?

All business requirements, Memoranda of Understanding, and Information Sharing Agreements are reviewed by the respective CBP program manager within the CBP Office of Field Operations, in consultation with the Office of Information Technology. Agreements involving PII are also generally approved by the CBP Privacy Officer, the Office of Chief Counsel, and DHS in accordance with procedures developed by the DHS Information Sharing Governance Board.

Responsible Officials

Deborah Augustin
Executive Director
Trade Remedy and Law Enforcement Division
Office of Trade
U.S. Customs and Border Protection

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

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

_____

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