Automated Commercial Environment Privacy Impact Assessment (PIA)

12/10/2018

USITC Privacy Program
privacy@usitc.gov

The Privacy Impact Assessment (PIA) assesses the risks to personally identifiable information (PII) of members of the public that is processed, used, maintained, or disseminated by the United States International Trade Commission (USITC).

Automated Commercial Environment Privacy Impact Assessment (PIA)

USITC PRIVACY PROGRAM

OVERVIEW

A Privacy Impact Assessment (PIA) must be conducted for United States International Trade Commission (USITC) systems that collect, use, process, maintain, or disseminate personally identifiable information (PII) about members of the public. A PIA is conducted to meet the requirements in the Office of Management and Budget (OMB) Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003, and to assess the risks to PII collected, used, processed, maintained, or disseminated by USITC.

1 SYSTEM, PROJECT, OR PROGRAM INFORMATION

1.1 What is the specific purpose of the USITC's use of the system and how does that fit with the USITC's mission?

The USITC participates in the Automated Commercial Environment (ACE) system, a system managed by the U.S. Customs and Border Protection (CBP), in order to obtain information relating to imports to and exports from the United States. The USITC collects this information to conduct statutorily mandated investigations and studies, including antidumping, countervailing duty, global safeguard, and intellectual property-related investigations, and industry and economic analysis.

2 INFORMATION COLLECTION

2.1 What types of personally identifiable information (PII) is collected? Please select all applicable items and provide a general description of the types of information collected.

- ☒ Name
- ☐ Mother's Maiden Name
- ☐ Social Security Number (SSN)
- ☐ Date of Birth
- ☐ Place of Birth
- ☒ Home Address
- ☒ Work Phone Number
- ☒ Work Email Address
- ☐ Logon Credentials (e.g. username, password)
- ☐ Driver's License Number
- ☐ Passport or Green Card Number
- ☐ Employee No. or other Identifier
- ☐ Tax ID Number

☐ Credit Card or Financial Account Number	☐ Biometric Records (e.g. fingerprints, photograph, etc.)	☐ Sexual Orientation
☐ Patient ID Number	☐ Sex or Gender	☐ Marital Status or Family Information
☒ Employment or Salary Record	☐ Age	☐ Race or Ethnicity
☐ Medical Record	☒ Home Phone Number	☐ Religion
☐ Criminal Record	☒ Personal Cell Number	☐ Citizenship
☐ Military Record	☒ Personal Email Address	☐Other:
☐ Financial Record	☒ Work Address	
☐ Education Record	☐ Physical Characteristics (eye or hair color, height, etc.)	☐None

Add Explanation: The USITC queries ACE records by product and may access information relating to an importer's, exporter's, or producer's name, organization, title or position, business role, address, telephone number, electronic mail address, Web site address, and Dun's number, as well as quantity and value information on imports and exports. Some contact information may be for the homes of individuals. Passport data is available in ACE, but the USITC does not query the system for this information.

2.2 About what types of people do you collect, use, maintain, or disseminate personal information? Please describe the groups of individuals.

The system contains records relating to an importer's, exporter's, or producer's name, organization, title or position, business role, address, telephone number, email address, Web site address, and Dun's number, as well as quantity and value information on imports and exports. Some contact information is for the homes of individuals (e.g. for sole proprietors). CBP collects the information in ACE. The USITC extracts only the information needed for investigations.

2.3 Who owns and/or controls the PII?

CBP manages ACE and owns the PII. The USITC obtains the information from CBP and other agencies that collect it. The USITC Office of Analysis and Research Services (OARS) manages the data for the USITC.

2.4 What specific laws, regulations, or policies authorize the USITC's collection of the PII? If the system collects Social Security Numbers (SSNs), please provide the authorities for this collection.

Statutory authority includes the following: 19 U.S.C. §§ 1330–1335, 1337, 1671 *et seq.,* 2151, 2213, 2251–54, 2436, 2482, 2704, 3204, 3353, 3372, 3381, 3804; and 7 U.S.C. § 624.

2.5 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected?

The USITC collects transaction-level information from ACE (e.g. import or export records of a specific item) and may aggregate this information as part of the investigation process.

2.6 Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Possible risks to the privacy of individuals' data include unauthorized access by both internal and external users, breaches of the system data, and the retention of records beyond the retention period or limit. Risks are mitigated through the use of access controls and other security controls based on guidance in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Records are retained and disposed of in accordance with retention requirements, as discussed in section 3.4.

3 USES OF THE SYSTEM AND THE INFORMATION

3.1 Describe all uses of the information. Describe how the information supports the USITC's mission or business function.

The USITC uses ACE records to conduct statutorily mandated investigations and studies, such as antidumping, countervailing duty, global safeguard, and intellectual property-related investigations and industry and economic analysis.

3.2 How can it be ensured that the PII is accurate, relevant, timely, and complete at the time of collection?

The USITC relies on CBP to verify the accuracy of the data at the time of collection. The USITC may notify CBP of any inaccuracies it identifies in the information exchanged.

3.3 How can it be ensured that only the minimum PII elements are collected?

USITC staff query data related to investigations and collect only the information needed for investigations. Additional PII elements (e.g. passport data) may be available in ACE, but the USITC does not collect information unless it pertains to an investigation.

3.4 What is the retention period for the system data? Has the applicable records disposition schedule been approved by the National Archives and Records Administration (NARA)?

Records are generally retained in accordance with USITC records schedule DAA-0081-2017-0003, item B1 (EDIS Master Files). Retention periods may be subject to interagency agreements and may vary depending on the case. Please refer to the CBP ACE PIA for information on the CBP's records retention information.

3.5 What methods are used to archive and/or dispose of the PII in the system?

Records are disposed of in accordance with NARA guidelines and USITC policy and procedures. Paper records are shredded, and records maintained on internal USITC electronic information systems are electronically removed. USITC electronic storage media that is no longer in service is purged in accordance with NIST guidelines for media sanitization. Disposal procedures for records in this system shall comply with requirements in applicable interagency agreements.

3.6 Will the data in the system be retrieved by a personal identifier?

Records may be retrieved by name. However, USITC staff typically search for records by querying for product or unit value.

3.7 If the answer is "yes" to the previous question, is the system covered by an existing Privacy Act System of Records Notice (SORN)?

ACE records are covered under SORN ITC-14, Import and Export Records, which was published in the Federal Register on September 27, 2017, at 82 FR 45046.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

4.1 With which internal components of the USITC is the information shared?

The USITC Office of Operations (Economics, Industries, Unfair Import Investigations, Tariff Affairs and Trade Agreements, Investigations, and Analysis and Research Services) and Office of General Counsel are the primary users of ACE data.

4.2 For each recipient component or office, what information is shared and for what purpose?

The USITC Office of Operations (Economics, Industries, Unfair Import Investigations, Tariff Affairs and Trade Agreements, Investigations, and Analysis and Research Services) and Office of General Counsel use ACE information to conduct statutorily mandated investigations and studies, including antidumping, countervailing duty, global safeguard, and intellectual property-related investigations, and industry and economic analysis.

4.3 How is the information transmitted or disclosed?

USITC users access ACE data through the ACE portal. Data are downloaded and saved to secure network folders. Because of the nature of the data, staff are discouraged from emailing data.

4.4 Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Possible risks to the privacy of individuals' data through internal sharing include unauthorized access by internal users and breaches of PII. Risks are mitigated through the use of access controls to limit access only to individuals with a need-to-know. All USITC employees and contractors are required to complete annual

information security and privacy awareness training to understand the requirements for safeguarding PII and to abide by rules of behavior for using USITC information systems.

5 EXTERNAL SHARING AND DISCLOSURE

5.1 With which external (non-USITC) recipient(s) is the information shared?

Records in this system may be disclosed to:

- The Office of the U.S. Trade Representative, CBP, and other agencies for safeguard and intellectual-property, and import injury related investigations;
- Representatives of parties to investigations under administrative protective order and/or judicial protective order, as necessary. Records in this system may be publicly disclosed as necessary in aggregated form that is not individually identifiable; and
- North American Free Trade Agreement panels and other tribunals, and U.S. courts reviewing trade remedy investigations, as necessary.

The USITC refers third party requests to CBP for access to ACE data. In accordance with the USITC MOU with CBP, and subject to certain exceptions, the USITC agrees not to disseminate information received from ACE to third parties without prior approval from CBP. The USITC primarily discloses aggregated data, but may disclose transaction level data in some cases.

5.2 What information is shared and for what purpose?

Please see the response to the previous question.

5.3 How is the information transmitted or disclosed?

The USITC transmits documents either by saving them to a compact disk (CD) and sending them via a courier or by encrypting and emailing the documents.

5.4 Are there any agreements with external entities concerning the security and privacy of the data once it is shared, such as a Memorandum of Understanding (MOU)?

The USITC and CBP completed an MOU on August 25, 2016 for the USITC's use of ACE.

5.5 Are privacy requirements included in contracts and other acquisition-related documents? If yes, please describe these requirements.

In accordance with USITC's MOU with CBP, the USITC is expected to complete a SORN and a PIA to address requirements of the Privacy Act and E-Government Act, respectively. The MOU also includes clauses to ensure that the USITC is responsible for safeguarding the integrity and confidentiality of the data, limiting access to employees and contractors who have an official need-to-know, and ensuring disclosures of data are consistent with applicable laws and policies.

5.6 What type of training is required for users from agencies outside USITC prior to receiving access to the information?

The USITC refers requests from third parties to access information to CBP.

5.7 Are there any provisions in place for auditing the recipients' use of the information?

The USITC MOU with CBP includes a provision to allow CBP to audit the USITC's security measures for accessing ACE and managing ACE data. The MOU also includes a provision that the USITC is responsible for maintaining safeguards to prevent unauthorized disclosure of data. CBP may decide to use additional methods to audit the use of data by other third parties.

5.8 Given the external sharing, please discuss any privacy risks that were identified and describe how they were mitigated.

Possible risks include unauthorized access and disclosure of the data. As noted, the USITC refers third party requests to access the data to CBP. Much of the ACE data that is disclosed to third parties is aggregate level data or under administrative protective order (APO), reducing the risks to individuals.

6 NOTICE

6.1 Was notice provided to the individual prior to collection of information? If notice was not provided, why not?

USITC has published SORN ITC-14, Import and Export Records, and has published this PIA to provide notice to individuals. CBP has completed a PIA for ACE and the Import Information SORN, DHS/CBP-001 to address these records. In addition, the ACE website includes a Privacy Act Statement

6.2 Do individuals have an opportunity and/or right to decline to provide information?

The below information from the CBP PIA for ACE addresses this question:

"U.S. law requires importers to provide CBP information that contains PII in conjunction with commercial entry documents submission that support importing commodities or merchandise in to or transit through the United States. Importer identity, manufacturer or supplier, and other parties involved in the import transaction and supply chain are necessary for commercial entry acceptance.

"Failure to provide required information will result in rejection of the commercial entry and the issuance of an order by CBP to remove the commodity from the territory of the United States. When importers submit the required information to ACE, they fulfill their legal requirements and they consent to how CBP will properly use this data."

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

As noted in the response to the previous question, U.S. law requires importers to provide the information that is collected in ACE.

6.4 Given the notice provided to individuals above, describe what privacy risks were identified and how they were mitigated.

Per CBP's PIA for the ACE, "[t]here is a risk that individuals may not know that their information is collected in ACE because many CBP forms do not have a Privacy Act Statement." In addition, individuals may not know that their information is used by USITC. This risk is mitigated by publication of this PIA, SORN ITC-14, the CBP ACE PIA, and the CBP IIS SORN.

7 INDIVIDUAL ACCESS AND REDRESS

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their information?

As outlined in SORN ITC-14, individuals may contact the USITC Privacy Act Officer to amend or request access to their records.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

SORN ITC-14 provides notice to individuals on the procedures for access and amendment.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Not Applicable. Individuals may seek amendment by contacting the USITC Privacy Act Officer.

7.4 Discuss any opportunities or procedures by which individuals can contest the accuracy of their information in the system or actions taken as a result of USITC reliance on information in the system.

Individuals may contest the accuracy of their data by submitting a request to the USITC Privacy Act Officer.

8 TECHNICAL ACCESS AND SECURITY

8.1 Who has access to the PII in the system?

PII in ACE can be accessed by USITC staff in the Offices of Operations and General Counsel who have a need-to-know and conduct statutorily mandated investigations and studies, including antidumping, countervailing duty, global safeguard, and intellectual property-related investigations, and industry and economic analysis.

8.2 Does the system use roles to assign privileges to users of the system?

There are two types of USITC ACE user roles: 1) Users with system and data access and 2) Users with access only to ACE data. Users with system and data access can login to the ACE system and view and download data. Users with data-only access do not have ACE accounts but receive ACE data from USITC employees who have ACE accounts.

8.3 What procedures are in place to determine which users may access the system and are they documented?

Users are granted access to ACE on a need-to-know basis. Before granting access to new users, the Office of Operations evaluates whether the potential users need access to the ACE system or to the data extracted from ACE. Some USITC users have ACE accounts and can view and download information from the system. Other USITC employees, however, do not have ACE accounts but may receive ACE data from USITC employees with ACE accounts. In addition, the Office of Operations annually reviews the ACE account information of USITC users and updates user account privileges where necessary.

8.4 What auditing measures and technical safeguards are in place to prevent misuse of data?

USITC does not currently audit users' use of ACE data. However, USITC implements numerous other security measures, as detailed in the response to question 8.5, to prevent misuse of data. In addition, CBP logs users' system activity and periodically reviews audit logs and ACE account users to identify potential misuse of data. Please refer to the CBP ACE PIA for more information.

8.5 How is the PII secured? What administrative, technical, and physical security safeguards are being used to guard against privacy risks?

USITC stores information downloaded from ACE in secure network folders and limits access to the folders to individuals with a need-to-know. Access to the USITC network requires use of authentication via a username and password or through a Personal Identity Verification (PIV) access card and Personal Identification Number (PIN). Paper records in this system are maintained in limited access spaces in locked offices in a building with restricted public access, patrolled by guards. Both standard and electronic locks are used to restrict access. In addition, all USITC system users must abide by the USITC Rules of Behavior, by which they agree to not access or use information that exceeds their job requirements and need-to-know.

8.6 Describe what privacy training is provided to users. How often do users complete the training?

All USITC personnel are required to complete annual privacy awareness training to understand their roles and responsibilities for protecting PII.

8.7 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured? If yes, does the system have a current authority to operate (ATO)?

CBP is responsible for conducting the ATO process for ACE. According to the ACE PIA, CBP planned to certify its ATO for the system upon publication of the ACE PIA.

8.8 Given access and security controls, describe what privacy risks were identified and describe how they were mitigated.

Privacy risks include unauthorized access to data and possible breaches of data. These risks are mitigated by granting access to users on a need-to-know basis and limiting the amount and types of data downloaded from ACE to the minimum necessary. In addition, all USITC system users must abide by the USITC Rules of Behavior, by which they agree to not access or use information that exceeds their job requirements and need-to-know.