# DataWeb Privacy Impact Assessment

9/17/2019

## USITC Privacy Program

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).

# DataWeb Privacy Impact Assessment

**USITC PRIVACY PROGRAM**

## OVERVIEW

The U.S. International Trade Commission (USITC) must conduct a Privacy Impact Assessment (PIA) for USITC systems that collect, use, process, maintain, or disseminate personally identifiable information (PII) about members of the public in order to comply with 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). The PIA assesses the risks to PII collected, used, processed, maintained, or disseminated by the 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 purpose support the USITC's mission?

The USITC Interactive Tariff and Trade DataWeb (hereafter referred to as "DataWeb") provides U.S. international trade statistics and U.S. tariff data to the public. Trade data are compiled from official data retrieved from the U.S. Bureau of the Census. U.S. import, export, and tariff information is available on a self-service, interactive basis. The USITC DataWeb responds to user-defined queries by integrating international trade statistics with complex tariff and customs treatment, and allows users to create and save customized country and product lists. DataWeb collects contact information from users and requires new users to create an account to access the data in the system.

## 2 INFORMATION COLLECTION

### 2.1 What types of PII are collected? Please select all applicable items and provide a general description of the types of information collected.

*PII* means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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

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

DataWeb is open to members of the public, and individuals access and use the system for a variety of purposes. When creating an account, users select one of the following as their organization: U.S. Government, Government (non-U.S.), International Trade or Financial Organization, Private Firm, Educational or Charitable Institution, or Personal Use Only.

## 2.3 Who owns and/or controls the PII?

The USITC.

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

DataWeb does not collect SSNs. Authority for DataWeb includes, but is not limited to, Section 332 of the Tariff Act of 1930 (19 U.S.C. § 1332) and Title VII of the Tariff Act of 1930 (19 U.S.C. §§ 1671-1677n).

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

Users are required to create a username and password to access DataWeb.

## 2.6 Given the amount, type, and purpose of information collected, 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 mission or a USITC business function.

USITC employees and/or contractors may access user account information to assist DataWeb users with account and/or system issues.

## 3.2 How can the USITC ensure that the PII is accurate, relevant, timely, and complete at the time of collection?

DataWeb relies on users to verify the accuracy of their data before creating new accounts to access the system. Users may login to their accounts or contact USITC to update their information if necessary.

## 3.3 How can the USITC ensure that only the minimum PII elements are collected?

When a new user creates a DataWeb account, the DataWeb registration page identifies the required and data fields. The required fields consist of data elements needed to sufficiently identify and contact a user (e.g. name, email address, organization name, username, password, etc.). The registration page requests only the information necessary for a user to establish an account and for USITC to contact users about their accounts.

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

Temporary. Delete/destroy when no longer needed for a business use. General Records Schedule 3.2, item 030, Information Systems Security Records, applies to these records.

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

The USITC does not currently track active users and therefore does not currently archive or dispose of inactive user account information because user accounts may be used rarely or unpredictably. However, user account information can be deleted or purged from DataWeb upon request.

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

Yes. Records are retrieved through searching by user's names and account information, such as email address.

### 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)?

SORN ITC-12, System Access Records, applies to user account records in DataWeb.

## 4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

This information is stored in a database and access is limited to the employees in the Office of Analysis and Research (OARS) and Office of the Chief Information Officer (OCIO). The OCIO conducts system and account maintenance tasks, and OARS provides DataWeb assistance.

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

DataWeb collects limited PII from users. When PII is needed to assist users (e.g. to address account maintenance or system questions), the office providing assistance has access to all information (such as name, contact, affiliation).

### 4.3 How is the information transmitted or disclosed?

The information is stored on a secured database and only accessible to OCIO information technology (IT) system administrators. Access is granted based on a "need to know" basis, and information is shared via secured network drives.

### 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. In addition, USITC system administrators are required to complete training that addresses their responsibilities as users with privileged access to DataWeb.

## 5 EXTERNAL SHARING AND DISCLOSURE

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

N/A. DataWeb user account information is not shared outside the USITC.

### 5.2 What information is shared and for what purpose?

N/A. DataWeb user account information is not shared outside the USITC.

### 5.3 How is the information transmitted or disclosed?

N/A. DataWeb user account information is not shared outside the USITC.

### 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)?

N/A. DataWeb user account information is not shared outside the USITC.

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

N/A. DataWeb user account information is not shared outside the USITC.

### 5.6 What type(s) of training is required for users from agencies outside the USITC prior to receiving access to PII?

N/A. DataWeb user account information is not shared outside the USITC.

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

N/A. DataWeb user account information is not shared outside the USITC.

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

N/A. DataWeb user account information is not shared outside the USITC.

## 6 NOTICE

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

The USITC's website includes a page on privacy (https://www.usitc.gov/privacy) which discusses USITC's privacy practices and the types of information the USITC website collects. The privacy page also includes a link to this document (DataWeb PIA). The USITC plans to develop a Privacy Act notice for the DataWeb registration page. The DataWeb registration page also includes a notice that describes how PII may be used. The privacy page also includes a link to the applicable SORN, ITC-12.

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

Individuals are not required to provide their information to DataWeb. However, if they do not provide the necessary information, they will be unable to create a user account and login to the system.

## 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?

By creating an account, users consent to the USITC's use of their data. Prior to creating a DataWeb account, potential users may read the disclaimer notice on the account creation page to understand how account information is used. If they object to how the data is used, they are not required to create a DataWeb account.

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

Potential risks with respect to notice include insufficient notice to users. Some users might not understand what types of information are collected by DataWeb and how this information is used. This risk is mitigated through the publication of this PIA on the USITC website and by including a link to the USITC Privacy Policy on the DataWeb webpage.

# 7 INDIVIDUAL ACCESS AND REDRESS

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

DataWeb users may access their information by logging in to the DataWeb website and may request updates to their information by submitting a help request through the USITC website. In addition, the USITC Privacy Act Rules (19 C.F.R. §§ 201.22-32) apply to all records in the USITC's Privacy Act systems of records. The rules describe the procedures by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures of those records that have been made by the USITC.

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

Notice may be provided through means such as a system of records notice (SORN), website privacy notice, or privacy notice on a form, etc. The DataWeb website includes a list of frequently asked questions (FAQs) with information on how to submit a help request. In addition, the USITC Privacy Act Rules detail procedures for amending records.

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

N/A. Users may amend their records by logging into their DataWeb account or by submitting a help request.

### 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.

DataWeb users may contest the accuracy of their information in DataWeb by submitting a help request via the USITC website to update their information. They may also submit a Privacy Act Request in accordance with the USITC Privacy Act Rules.

## 8 TECHNICAL ACCESS AND SECURITY

### 8.1 Who has access to the PII in the system?

The USITC IT system administrators within OCIO can access user account data. Limited scope information may be shared with staff in OARS to assist in account maintenance.

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

There are two primary DataWeb roles: public and system administrator. All public users are granted the same level of access; these users can query and access trade data in the system. System administrator roles are granted only to USITC staff based on. "need to know". USITC administrators are granted access to DataWeb to perform system administration tasks (e.g. updating the website and software, account maintenance, etc.).

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

USITC employees are granted system administrator accounts based on their job responsibilities and "need to know". All members of the public can create public accounts.

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

Users are granted access to information in DataWeb on a "need to know" basis and are granted the least privilege needed to conduct their duties. DataWeb implements auditing controls in accordance with the NIST 800-53 guidance to track user behavior and identify misuse of the system.

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

DataWeb implements security controls in accordance with the NIST SP 800-53 guidance. These controls are designed to minimize unauthorized access, use, and dissemination of PII.

## 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. In addition, users with privacy responsibilities are required to complete role-based training.

## 8.7 Are all information technology 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)?

DataWeb is part of the USITC's network which has received an ATO.

## 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 through the implementation of security controls in accordance NIST SP 800-53 guidance.