# Electronic Document Information System (EDIS) Privacy Impact Assessment (PIA)

11/16/2018

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).

# Electronic Document Information System (EDIS) Privacy Impact Assessment (PIA)

USITC PRIVACY PROGRAM PRIVACY@USITC.GOV

## OVERVIEW

A Privacy Impact Assessment (PIA) must be conducted for 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 Electronic Document Information System (EDIS) manages documents comprising the official record of all investigations conducted by the USITC in its quasi-judicial role. EDIS is a repository for information owned by the Office of the Secretary and supports the operations of the Office of Investigations, which processes investigative documents; the Office of the General Counsel, which uses the system for litigation support and legal research; the Office of Unfair Import Investigations, which represents the public in intellectual property investigations; the Administrative Law Judges; and other USITC offices, which use the system for legal and other research. EDIS provides access to external users seeking to file documents in response to a specific investigation or to search for and retrieve documents available for public access.

# 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
- ☐ 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 (eye or hair color, height, etc.)
- ☐ Sexual Orientation
- ☐ Marital Status or Family Information
- ☐ Race or Ethnicity
- ☐ Religion
- ☐ Citizenship
- ☐ Other:
- ☐ None

**Explanation**:

EDIS collects legal documents or notes (e.g. motions, briefs, opinions, complaints, or petitions), resumes or CVs of individuals involved with litigation, comments filed by the public on investigations, and system login information about users. Many documents contain the name of an individual representing/participating in a USITC investigation and may include the individual's employment affiliation (e.g. the name of the firm the individual is representing). Some of these documents may be publicly available. When external users create accounts, they provide contact information such as address, phone number, and email address. Users will typically provide a work address, phone number, and email address but might submit a personal address, phone number, or email address instead.

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

EDIS collects information on members of the public, USITC employees and contractors, vendors, suppliers, individuals involved in cases before the USITC (e.g. representatives of companies or law firms), and contacts at other agencies or government entities (e.g. Congress, U.S. Department of Commerce, and Federal, state, and local agencies). This information includes both account information for users accessing EDIS and information included in documents submitted through EDIS.

## 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.

Statutory authority includes the following: 19 U.S.C. §§ 1330–1335, 1337, 1671 *et seq.,* 2151, 2213, 2251–2254, 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?

New users accessing EDIS are prompted to create usernames and passwords, which are used to authenticate users accessing the system.

## 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 functions.

EDIS manages documents related to the USITC's investigatory roles. EDIS supports the USITC's investigative processes and the functions of the Offices of the Secretary, Investigations, General Counsel, Unfair Import Investigations, Administrative Law Judges and others.

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

EDIS relies on users to verify the accuracy of their data before creating a new account to access the system. Users may contact the EDIS Help Desk to fix errors in their account information. Similarly, if a user files a document and notices it contains an error, the user can contact the USITC Docket Services Division to remove the error.

The Docket Services Division performs additional assessments to ensure potential errors are identified and addressed. The division reviews EDIS accounts annually to determine if accounts need to be deactivated and coordinates with the relevant USITC offices to determine if any user's privileges need to be modified. In addition, accounts are automatically deactivated after 180 days of inactivity. Accounts are categorized as inactive after 180 days of inactivity. After an additional 180 days of inactivity, accounts are disabled.

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

When a new user creates an EDIS account, the EDIS registration page identifies the required and optional data fields. The required fields consist of data elements needed to sufficiently identify and contact a user (e.g. name, email address, office address, 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 account or for information relating to a case or 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)?

EDIS records are retained and disposed of in accordance with NARA Records Schedule Number DAA-0081-2017-0003-0001.

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

Hard copy files are destroyed. Electronic documents can be archived in the system; these documents may be retrieved by a limited number of EDIS users with privileged accounts. In order to fully delete a document from EDIS, it must be removed manually from the file server.

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

Yes. Records are retrieved through searching by name, email address, employment status, legal documents, or user name/ID.

### 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 the user account records in EDIS. PII contained in investigation documents is typically not retrieved by a personal identifier. As a result, USITC has determined that a SORN is not necessary for these records.

## 4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

Documents filed in EDIS support the USITC's investigative processes and are accessed by the Offices of the Secretary, Investigations, General Counsel, Unfair Import Investigations, Administrative Law Judges and others.

The Offices of the Secretary and Chief Information Officer (CIO) access user account records to manage user account privileges and to audit user activity.

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

Each USITC office accesses and uses documents in EDIS based on the corresponding need. All internal EDIS users (USITC employees and contractors) can access documents categorized as Public (documents accessible by the general public) or Limited (public transcripts of USITC proceedings that are withheld from public access for 45 days following court activity). Permission to view documents with security rating above Public are granted based on need-to-know.

The Offices of the Secretary and CIO access user account records to manage user account privileges and audit user activity.

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

Documents can be viewed and downloaded electronically from EDIS, distributed via compact disc (CD), or printed from EDIS and transmitted via paper copy.

### 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 EDIS.

# 5 EXTERNAL SHARING AND DISCLOSURE

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

Not Applicable. EDIS does not share PII with external entities.

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

Not Applicable. EDIS does not share PII with external entities.

## 5.3 How is the information transmitted or disclosed?

Not Applicable. EDIS does not share PII with external entities.

## 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)?

Not Applicable. EDIS does not share PII with external entities.

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

Not Applicable. EDIS does not share PII with external entities.

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

Not Applicable. EDIS does not share PII with external entities.

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

Not Applicable. EDIS does not share PII with external entities.

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

Not Applicable. EDIS does not share PII with external entities.

# 6 NOTICE

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

The USITC 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 the EDIS PIA. USITC plans to develop a Privacy Act notice for the EDIS registration page.

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

Individuals are not required to provide their information to EDIS. 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?

Prior to creating an EDIS account, potential users may read the EDIS Terms of Use Agreement and applicable SORN (ITC-12, System Access Records) to understand how EDIS account information is used. If they object to how the data is used, they are not required to create an EDIS account, and thus would not consent to the use of their data by EDIS.

## 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 EDIS 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 EDIS webpage.

# 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?

EDIS users may access their information by logging in to the EDIS website and may request updates to their information by contacting the EDIS Help Desk.

In addition, the USITC Privacy Act Rules apply to all records in systems of records maintained by the USITC that are retrieved by an individual's name or other personal identifier. They 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 by the USITC.

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

The EDIS website includes links to the EDIS User Guide, which provides instructions for updating account information, and the EDIS Help Desk, which users can contact to update their information.

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?

Not Applicable. Users may amend their records by contacting the EDIS Help Desk.

### 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.

EDIS users may contest the accuracy of their information in EDIS by contacting the EDIS Help Desk 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?

EDIS user account information is accessible only by the Office of Secretary staff authorized to conduct account administration tasks (e.g. creating an account, modifying account information, etc.) and by the Office of the Chief Information Officer (OCIO) for system maintenance purposes. All EDIS users can access incidental PII that appears in publicly available documents field in EDIS.

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

Users are assigned role-based privileges based on need-to-know and their job responsibilities (for USITC staff). In addition, USITC information system administrators are granted access to EDIS to perform system administration tasks (e.g. updating the website and software, removing inactive accounts, etc.).

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

The EDIS User Guide describes procedures for granting users access to the system. Users are granted access to EDIS based on need-to-know and their job responsibilities (for USITC staff). New users must agree to the EDIS Terms of User Agreement before establishing an account.

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

As noted previously, users are granted access to information in EDIS on a need-to-know basis and are granted the least privilege needed to conduct their duties. EDIS 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?

EDIS 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.

## 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)?

EDIS has a current ATO and addresses information security requirements in accordance with the Federal Information Security Modernization Act (FISMA) and the relevant policies and guidance, such as NIST SP 800-53.

## 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 a data loss prevention (DLP) tool and security controls in accordance NIST SP 800-53 guidance. The USITC develops and maintains a Plan of Action & Milestones (POA&M) for EDIS to address security controls that are not implemented or operating effectively.