Investigations System Privacy Impact Assessment

11/7/2023

USITC Privacy Program

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

Investigations System Privacy Impact Assessment

USITC PRIVACY PROGRAM

OVERVIEW

Under the E-Government Act of 2002, the USITC must conduct a PIA before developing or procuring any information technology (IT) for USITC systems or projects that collect, process, use, maintain, or disseminate PII about members of the public. Office of Management and Budget (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003) provides implementation guidance to agencies as they assess the risks to PII collected, used, processed, maintained, or disseminated by IT systems or projects.

1 SYSTEM, PROJECT, OR PROGRAM INFORMATION

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

The Investigations System (IS) is composed of two subsystems: the Electronic Document Information System (EDIS) and the Investigations Database System (IDS).

EDIS is a repository for documents comprising the official record of all USITC investigations and includes data and statistics related to these investigations. EDIS users file documents on EDIS, including: (1) legal documents such as motions, briefs, complaints, petitions, notices, or orders; (2) resumes or CVs of individuals involved with USITC investigations; and (3) comments from members of the public. In addition, EDIS users can use EDIS to search for and retrieve documents filed in an investigation and certain information about filed documents.

IDS is the official repository for Commission investigation-related data. It is a peer to EDIS, but unlike EDIS, IDS does not manage any documents. The Commission uses IDS to meet its statutory, investigative, and other information needs. This includes information about companies, other organizations, and individuals who are directly involved with statutory investigations (i.e., antidumping, countervailing duty, safeguard, unfair import, and fact-finding investigations).

Multiple USITC offices use IS for various functions related to Commission investigations. These offices include: the Offices of the Commissioners, the Office of the Administrative Law Judges, as well as the Offices of Operations, Analysis and Research Services, Economics, Industry and Competitiveness Analysis, Investigations, External Relations, Tariff Affairs and Trade Agreements, the General Counsel, Unfair Import Investigations; and the Secretary.

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.

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 (eye or hair color, height, etc.)
- ☐ Sexual Orientation
- ☐ Marital Status or Family Information
- ☐ Race or Ethnicity
- ☐ Religion
- ☐ Citizenship
- ☒ Other:

JCC JCIUW

- ☐ None

Explanation:

IS collects data on Commission investigations. The data collection for both IDS and EDIS includes PII stored as account registration, system login information, and incidental PII that may appear in documents or online (e.g., names of individuals involved in an investigation). Additionally, EDIS system login information may contain the name of the individual, employment affiliation (e.g., the name of an EDIS filer's employer), and contact information (e.g., address, phone number, and email address). EDIS typically collects work-related contact information, but in some cases, it may collect personal contact information when an EDIS user chooses to supply it. For example, the USITC does not require EDIS users to supply personal contact information (e.g., personal email address, cell phone, home address), but some small businesses may choose to use this as their contact information. EDIS also collects security question information at registration, such as the name of the user's past school or street name.

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

EDIS collects information on all EDIS users, including members of the public; USITC employees and contractors; vendors; suppliers; individuals involved in investigations 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 PII included in documents submitted through, and stored on, EDIS.

IDS collects user account information for USITC staff who manage or access the system and maintains and may display information on members of the public involved in an investigation.

2.3 Who owns or controls the PII?

The USITC owns and controls the IS subsystems (EDIS and IDS) that collect and store the PII.

2.4 What specific laws, regulations, or policies authorize the collection of the PII? If the system collects SSNs, please provide the authority 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, 3804; 4571-4574; and 7 U.S.C. § 624. IS does not collect SSNs.

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 EDIS users must create unique usernames and passwords to access EDIS, which uses the usernames and passwords to authenticate users. EDIS does not generate or derive any additional data using their account information. IDS accounts are created based on USITC staff contact information (e.g., email address) that exists as part of each user's USITC network account. IDS does not generate or derive any additional data using their account information.

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

Possible risks to the privacy of PII 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 activities. EDIS supports the USITC's investigative processes and the functions of the Offices of the Secretary, Investigations, the General Counsel, Unfair Import Investigations, Administrative Law Judges, and others.

IDS is the official repository for Commission investigation-related data. It is a peer to EDIS, but unlike EDIS, IDS does not manage any documents. The Commission uses IDS to meet its statutory, investigative, and other information needs.

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

IS relies on users to verify the accuracy of their data before creating a new account to access the system.

For EDIS accounts, 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 Office of the Secretary, Docket Services Division ("Docket Services") for assistance. Docket Services performs additional assessments on filed documents to identify and address potential errors.

For account management, user passwords expire automatically after 180 days, and the account is set to "Inactive" if the password is not reset. EDIS accounts are set to "Disabled" after one full year of non-use. For internal USITC staff, Docket Services disables the accounts of departing staff as part of their out-processing. They also review EDIS internal accounts annually and coordinate with the relevant USITC offices to determine if any user's privileges need to be modified.

OCIO creates IDS accounts and administers access to the system for ITC staff who need access as part of their job duties. OCIO creates IDS accounts with staff-provided usernames. Users can verify the accuracy of their information upon providing it and can request that OCIO make updates, if needed.

3.3 How can the USITC ensure 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 users about their accounts (e.g., name, email address, office address, username, password, security questions).

IDS accounts are created based only on the information needed to authenticate the users, which includes the user's name and logon credentials.

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)?

Both EDIS and IDS user account records are covered by NARA General Records Schedule 3.2, item 030, Information Systems Security Records.

EDIS records (other than user account data) are retained and disposed of in accordance with NARA Records Schedule Number DAA-0081-2017-0003.

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

The USITC destroys hard copies of its files. It archives electronic documents in EDIS; these archived documents may be retrieved by a limited number of EDIS users with privileged accounts. In order to delete a document from EDIS, it must be removed manually from the file server. IDS user accounts are connected to a user's USITC IT account, and these accounts are archived once a user leaves the agency.

3.6 Will the records in the system be retrieved by PII?

Yes. EDIS user account records can be retrieved by internal EDIS users with administrative privileges through searching by username/ID, first and/or last name, and employment status. EDIS document records can be retrieved by EDIS users using the name or the employment status of the person identified as the filer of the document. IDS user account records are retrieved by IDS administrators via name or email address. IDS investigation records can be retrieved by users based on the names of certain USITC staff or case managers assigned to an investigation.

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)?

The SORN ITC-12, System Access Records, applies to the user account records in EDIS and IDS. The USITC does not typically retrieve investigation documents by PII. As a result, USITC has determined that a SORN is not necessary for the investigation records stored in EDIS.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

IS supports multiple USITC offices which use the system for various functions related to investigations. These offices include: the Offices of the Commissioners; the Office of the Administrative Law Judges; as well as the Offices of Operations, Analysis and Research Services, Economics, Industry and Competitiveness Analysis, Investigations, External Relations, Tariff Affairs and Trade Agreements, the General Counsel, Unfair Import Investigations, and the Secretary.

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

Each USITC office accesses and uses documents in IS 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 other than Public/Limited are granted on a need-to-know basis.

The Office of the Secretary and OCIO access EDIS and IDS user account records to manage user account privileges and audit user activity.

4.3 How is the information transmitted or disclosed?

Document information can be viewed from the EDIS user interface and documents can be downloaded electronically from EDIS or printed from EDIS and transmitted via paper copy. Documents and their metadata can also be retrieved through automation via the EDIS Data Web Service using a formatted URL to construct a query which returns results in XML format.

Investigation data can be viewed from the IDS user interface or downloaded in JSON format from the Data.gov website. Data for investigations prior to October 2008 can be downloaded in Microsoft Excel spreadsheet format.

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 IS.

5 EXTERNAL SHARING AND DISCLOSURE

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

Not applicable. IS does not share PII with external entities.

5.2 What information is shared and for what purpose?

Not applicable. IS does not share PII with external entities.

5.3 How is the information transmitted or disclosed?

Not applicable. IS 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. IS 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. IS does not share PII with external entities.

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

Not applicable. IS does not share PII with external entities.

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

Not applicable. IS 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. IS does not share PII with external entities.

6 NOTICE

6.1 Is notice provided to the individual prior to collection of information? If advance notice is not provided, why not?

The USITC website includes a page on privacy (https://www.usitc.gov/privacy) which discusses USITC's privacy practices, the types of information the USITC website collects. The privacy page also includes a link to the USITC's PIAs. The EDIS registration and login pages include a Privacy Act statement. For internal IDS users, users are provided notice via the onboarding forms they complete prior to working at USITC.

6.2 Do individuals have an opportunity or right to decline to provide their PII?

For EDIS, both external (members of the public) and internal (USITC staff) users must create an EDIS account to access information on the system and submit documents If they do not provide the necessary information, they will be unable to create a user account and login to the systems. External IDS users do not need an account in order to access information in IDS.

6.3 Do individuals have an opportunity to consent to particular uses of their PII, 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 they would not consent to the use of their data by EDIS.

For IDS accounts, when USITC staff members begin working at USITC, the agency creates an IT account for them, and the user consents to use of their PII and agrees to abide by the USITC IT rules of behavior, which apply to IDS.

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 IS 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 and IDS webpages.

7 INDIVIDUAL ACCESS AND REDRESS

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

Individuals may request corrections or amendment to inaccurate PII in EDIS or IDS by submitting a Privacy Act request in accordance with the USITC Privacy Act Rules. For users with EDIS accounts, they may also contact the EDIS Help Desk or OCIO to correct or amend PII.

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

The IS PIA provides notice to individuals regarding access and amendment procedures. The EDIS Privacy Act Statement refers to the applicable SORN, ITC-12, which describes procedures for accessing and amending PII.

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 user account information by contacting the EDIS Help Desk or OCIO.

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 request an update to their information. They may also submit a Privacy Act Request in accordance with the USITC Privacy Act Rules. IDS users can contact the OCIO to contest the accuracy of their information.

8 TECHNICAL ACCESS AND SECURITY

8.1 Who has access to the PII in the system?

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

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, disabling inactive accounts).

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

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

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

As noted previously, internal users are granted access to information in IS on a need-to-know basis and are granted the least privilege needed to conduct their duties. IS implements auditing controls in accordance with the NIST SP 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?

IS 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 Is the USITC following all IT security requirements and procedures required by Federal law to ensure that PII is

appropriately secured? If yes, does the system have a current authority to operate (ATO)?

IS 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 potential 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 with NIST SP 800-53 guidance.