USITC.gov Website Applications Privacy Impact Assessment

9/10/2025

USITC Privacy Program

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

USITC.gov Website Applications Privacy Impact Assessment

USITC PRIVACY PROGRAM

OVERVIEW

Under the E-Government Act of 2002, the U.S. International Trade Commission (USITC or Commission) 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. 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) provides implementation guidance on how agencies should assess the risks to PII that they collect, use, process maintain, or disseminate.

This document includes guidance to help complete the PIA. Upon completion of this form, please submit it to privacy@usitc.gov for review by the USITC Privacy Program. Once the PIA has been reviewed and approved, USITC will publish it on the USITC website, unless doing so would raise security concerns.

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 fit with the USITC's mission?

The United States International Trade Commission utilizes various services to manage its website, www.usitc.gov. This PIA addresses the following web applications used by the USITC’s public website and its applications on the usitc.gov domain to analyze user traffic, provide website updates to users, and authenticate users: Google Analytics, GovDelivery, and Login.gov. Google Analytics gathers data on web traffic for users visiting the website and web applications. GovDelivery allows website users to provide their contact information and receive notifications when the USITC website has been updated. Login.gov is used to authenticate users accessing USITC web application services such as DataWeb and Electronic Document Information System (EDIS).

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.

Personally Identifiable Information (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:

☐None

Explanation:

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

The USITC.gov web applications collect information on individuals accessing the USITC.gov website and logging into various website services. Visitors to the websites include members of the public as well as USITC staff, its contractors, and employees of other government agencies.

2.3 Who owns and/or controls the PII?

USITC controls the PII it collects. Some data may be managed by other organizations such as the General Services Administration (GSA), which manages Login.gov. USITC subscribes only to Login.gov's authentication service which collects authentication information (e.g. username, password, email address) on individuals with Login.gov accounts. USITC can access email addresses that users provide through their Login.gov accounts.

USITC does not subscribe to Login.gov's identity proofing/verification service that collects information needed to conduct identity proofing activities for individuals. As a result, USITC does not collect information used in this process (e.g., driver's license, SSN, etc.).

The vendor of GovDelivery, Granicus, owns and controls the PII acquired when users register to create a GovDelivery account. USITC controls PII associated with GovDelivery administrative accounts for USITC staff. In addition, individuals can create accounts within GovDelivery. USITC administrators can access GovDelivery user account information which includes name, email address, and phone number (optional). Users must provide a name and email address to create a GovDelivery account; they have the option to provide a phone number but are not required to do so.

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.

19 U.S.C. 1331(a)(1)(A)(iii). USITC does not collect SSNs as part of Login.gov. USITC understands that Login.gov itself does not collect SSNs as part of the services it provides to USITC. USITC subscribes only to Login.gov's authentication service which collects authentication information (e.g. username, password, email address) of individuals with Login.gov accounts. USITC can access email addresses that users provide through their Login.gov accounts.

USITC does not subscribe to Login.gov's identity proofing/verification service which collects information needed to conduct identify proofing activities for individuals. As a result, USITC does not collect information used in this process (e.g., driver's license, SSN, etc.).

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 create login credentials, including passwords, when creating accounts for Login.gov to access EDIS and DataWeb on the USITC.gov website. Users also create authentication credentials to access GovDelivery via the USITC website.

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. 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 Commission business function.

USITC uses information collected through the USITC.gov web applications for purposes such as analyzing aggregated user traffic, providing website updates to users, and authenticating users. Google Analytics gathers anonymous data on web traffic for users visiting the website and web applications. No PII is collected or analyzed through Google Analytics. GovDelivery allows website users to provide their contact information and receive notifications when the USITC website has been updated. This information is managed by the vendor, Granicus, and is not used directly by the USITC. Login.gov is used to authenticate users accessing USITC web application services such as DataWeb and EDIS. The USITC collects the email addresses associated with the users' Login.gov account and associates them with their DataWeb or EDIS account for reference purposes only.

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

USITC relies on the users that access the website to verify the accuracy of their data when providing their information. For instance, when users create accounts, they provide their contact information for use in services such as GovDelivery and Login.gov. USITC relies on the accuracy of user data provided by these services. When users associate their Login.gov accounts to their application accounts (e.g., EDIS and/or DataWeb accounts), USITC asks the users to verify the accuracy of their contact information that is used for both Login.gov and the application accounts. Users confirm this information through a link that is sent to their email accounts.

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

USITC collects only the information necessary for the creation of user accounts and to track user activity on the website.

USITC subscribes only to Login.gov's authentication service which collects authentication information (e.g. username, password, email address) on individuals with Login.gov accounts. These data elements are the minimum necessary items used by USITC for authentication purposes. Since Login.gov is managed by GSA, USITC relies on GSA to collect the minimum information necessary for authentication purposes.

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)?

User account records are covered by NARA General Records Schedule 3.2, item 030, Information Systems Security Records. USITC complies with the foregoing records schedule.

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

For GovDelivery, users can request deactivation of their accounts and removal of their account information (e.g. email address) through the service. Google Analytics does not collect PII on website users. GSA manages archiving and disposal of Login.gov account data (e.g. email address and authentication information).

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

Yes. User account records and records of user activity may be retrieved via user account name or 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)?

The SORN ITC-12, System Access Records, applies to the user account records collected by the USITC.gov website. GSA SORN GSA/TTS-1, Login.gov applies to Login.gov records.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

The USITC Office of the Chief Information Officer (OCIO) manages the USITC.gov web applications and the data stored by the system. The Office of External Relations can access some data in GovDelivery, and the Office of Operations can access data in Google Analytics.

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

The OCIO uses data collected from Google Analytics to analyze aggregated website traffic but collects no PII through this service. USITC analyzes aggregated website traffic to understand trends on the types of information on the website that is viewed by site visitors. The GovDelivery notification service collects first name, last name and email address to provide notifications to users about updates to the USITC's public website content. The OCIO receives user data to include an email address from Login.gov to authenticate users to USITC web services. The Office of External Relations accesses data from GovDelivery to manage information on external points of contact. Office of Operations accesses Google Analytics data to analyze website data.

4.3 How is the information transmitted or disclosed?

OCIO system administrators have administrator access to view and update data collected by these website applications to analyze information collected, provide information on the website to users, and to conduct account management activities (e.g., creating, deleting accounts, etc.)

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 the data.

5 EXTERNAL SHARING AND DISCLOSURE

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

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties.

5.2 What information is shared and for what purpose?

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties.

5.3 How is the information transmitted or disclosed?

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties.

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. USITC does not share information collected via the USITC.gov web applications with any third parties.

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

USITC has entered into an Interagency Agreement (IAA) with GSA for use of Login.gov. USITC's acquisition documents include provisions related to privacy compliance and protection of PII, where applicable.

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

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties. USITC expects users of outside entities accessing PII to complete foundational privacy training.

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

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties, so auditing is not needed.

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

Not applicable. USITC does not share information collected via the USITC.gov web applications with any third parties.

6 NOTICE

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

The USITC.gov website includes privacy notices linked to the www.usitc.gov/privacy page. The Web Privacy Notice (Web Privacy Notice | United States International Trade Commission) provides notice on information collected via the website. In addition, this PIA provides notice to users.

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

Individuals are not required to provide their information to USITC. However, if they do not provide their information to establish either a Login.gov or GovDelivery account, they will be unable to use the applicable website services.

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 providing their information for use for the various USITC.gov web applications, potential users may read the privacy notice on the web site as well as this PIA. If they object to how the data is used, they are not required to provide their information, and thus they would not consent to the use of their data by the web applications.

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 the USITC.gov website applications and how this information is used. This risk is mitigated through the publication of the web privacy notice (Web Privacy Notice | United States International Trade Commission) and this PIA.

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?

Individuals may request corrections or amendment to inaccurate PII collected by USITC.gov website applications by submitting a Privacy Act request in accordance with the USITC Privacy Act Rules.

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

This PIA provides notice to individuals regarding access and amendment procedures. In addition, the applicable SORNs, ITC-12 and GSA/TTS-1, describe 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 submitting a Privacy Act 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.

Users may 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?

Information collected through the website applications is accessible only by USITC OCIO staff who manage the system and by some users in Office of External Relations who can access data in GovDelivery.

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

USITC staff users are assigned role-based privileges based on need-to-know and their job responsibilities. In addition, USITC information system administrators are granted access to the system to perform system administration tasks (e.g., updating the website and software). In GovDelivery, there are three administrative roles: Topic, Group, and Account. They provide the ability to add to and edit the list of available topics, to create and edit topic groups, and to manage user administrative accounts and generate reports, respectively.

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

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

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

The USITC.gov website applications implement auditing controls in accordance with NIST SP 800-53 guidance to track user behavior and identify misuse of the system. USITC staff can access GovDelivery audit information for successful authentications to administrative accounts to monitor account usage.

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

USITC implements security controls in accordance with 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)?

The USITC.gov website applications are part of the International Trade Commission Network (ITCNET) system, which has a current ATO. In addition, Login.gov and GovDelivery have ATOs as part of GSA's Federal Risk and Authorization Management Program (FedRAMP) security authorization program.

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 with NIST SP 800-53 guidance.