United States International Trade Commission Public Guest Wireless Network Privacy Impact Assessment (PIA)

4/29/2025

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).

United States International Trade Commission Public Guest Wireless Network Privacy Impact Assessment (PIA)

USITC PRIVACY PROGRAM

Record of Template Changes

Version	Date	Description	Author
1.0	October 2017	New Template	Mike O'Rourke
2.0	July 2018	Updated the Approval Section	Mike O'Rourke

OVERVIEW

A Privacy Impact Assessment (PIA) must be conducted for the 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* (Sep. 26, 2003), and to assesses the risks to PII collected, used, processed, maintained, or disseminated by the USITC.

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, the USITC will publish it on its 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 it fit with the USITC's mission?

The USITC Guest wireless internet network provides wireless internet services to any person who is physically present in the headquarters (HQ) building for hearings and other permissible activities. The USITC staff (employees and contractors) may also use the guest wireless network.

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
- ☐ 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: Only the first name is collected during a one-time-use account registration. Email address requested allows for the receipt of a username and password and can be either personal or official email address.

2.2 What groups of individuals do you collect, use, maintain, or disseminate personal information? Please describe them.

The guest wireless network collects information on any individuals accessing the USITC guest wireless network while at the USITC HQ building. Individuals may include people attending hearings at the HQ building, other visitors to the building, and the USITC staff who access the network via their personal devices.

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.

19 U.S.C. 1331(a)(1)(A)(iii). This system 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?

The guest wireless system creates a username and password when guest users attempt to access the network.

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.

The USITC uses information collected through the guest wireless system to grant and track user access of the system to ensure compliance with the USITC rules of use of IT resources.

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 the users that access the guest wireless network to verify the accuracy of their data when creating accounts for use of the network.

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

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

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.

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

Guest user accounts created during guest wireless system onboarding expire after 90 days, with expired accounts purged every 15 days.

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

Yes. User contact information (e.g., user name) and records of user activity may be retrieved from the guest wireless portal via user 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 in the guest wireless system.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

4.1 Which internal components of the Commission is the information shared with?

The USITC Office of the Chief Information Officer (OCIO) manages the guest wireless network and the data stored by the system. User records are not shared internally with other USITC components.

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

The OCIO manages user access and user account data to ensure the system is used in accordance with appropriate rules. OCIO uses data in the system for account maintenance purposes (e.g., creating, deleting accounts, etc.).

4.3 How is the information transmitted or disclosed?

The OCIO system administrators have administrator access to view and update data in the system in order 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 the USITC information systems. In addition, the USITC system administrators are required to complete training that addresses their responsibilities as users with privileged access to the system.

5 EXTERNAL SHARING AND DISCLOSURE

5.1 Which external (non-USITC) recipient(s) is the information shared with?

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

5.2 What information is shared and for what purpose?

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

5.3 How is the information transmitted or disclosed?

Not applicable. The USITC does not share information collected via the guest wireless network 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. The USITC does not share information collected via the guest wireless network with any third parties.

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

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

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

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

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

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

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

Not applicable. The USITC does not share information collected via the guest wireless network with any third parties.

6 NOTICE

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

The login page for the guest wireless system includes a Privacy Act Statement. In addition, this PIA provides notice to users of the wireless system.

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

Individuals are not required to provide their information to the USITC. However, if they do not provide their information, they will be unable to use the guest wireless 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?

Before gaining access to the guest wireless system, potential users must read and consent to the terms of use on the USITC web page to create a user account. If the person objects to any of the terms, including how the data is used, he or she may decline to consent and will not be required to proceed with the creation of an 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 may not understand what types of information are collected by the guest wireless system and how this information is used. This risk is mitigated through the publication of the Privacy Act statement on the login page and this PIA on the USITC website.

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 in the guest wireless system by submitting a Privacy Act request in accordance with the USITC Privacy Act Rules. Individuals may not request an update of their information directly through the guest wireless system, as only first name and email address of users are collected when accounts are created. Users create an account by inputting their first name and email address. The guest wireless system then generates a unique username and password and sends it to the user so they can access the wireless network. The system does not provide an account management option for users to update their information.

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 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 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's 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?

Guest wireless account information is accessible only by the USITC OCIO staff who manage the system.

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 the USITC staff). In addition, the USITC information system administrators are granted access to the system 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?

Any individual physically at the USITC HQ may access the guest wireless network after agreeing to the terms of use, including the acceptable use policy outlined on the login page.

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

The guest wireless system implements auditing controls in accordance with NIST SP 800-53 guidance to track user behavior and identify misuse of the system. Administrators may disable accounts of users who violate the acceptable user policy.

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

The 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 guest wireless network is part of the International Trade Commission Network (ITCNET) system, which has a current 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 a data loss prevention (DLP) tool and security controls in accordance with NIST SP 800-53 guidance.