USITC Freedom of Information Act and Privacy Act Privacy Impact Assessment

9/16/2025

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 Freedom of Information Act and Privacy Act Privacy Impact Assessment

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.

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 USITC Office of the Secretary (OSE) manages the USITC's Freedom of Information Act (FOIA) and Privacy Act request and appeal processes. Through the FOIA process, members of the public may submit requests to the USITC for it to publicly release information that the USITC maintains. Through the Privacy Act request process, individuals may submit requests to the USITC for information that the USITC maintains about them. Individuals who submit a FOIA or Privacy Act request may also submit an appeal of any adverse determinations for those requests.

OSE uses the ArkCase FOIA service, a cloud-based service, to manage the FOIA process. Members of the public can submit FOIA requests and appeals through the ArkCase service, and OSE uses ArkCase to track and respond to requests, upload files, and manage appeals. OSE uses ArkCase to receive and upload documents, create correspondence to the requestor, redact responsive documents, issue final determinations and any releasable documents to the requestors, manage payments for FOIA services, and manage appeals. Requestors can look up FOIA requests and appeals and track the status of specific FOIA requests and appeals through ArkCase. Requestors can input the FOIA number to check the status of a request or appeal (e.g., received, pending, in process).

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

Explanation: Individuals submitting FOIA requests or appeals must provide their name, mailing address, and phone number. Individuals submitting Privacy Act requests must provide their full name, citizenship status, current address, date and place of birth, and dates of employment with the USITC (if applicable), and submit verification of their identity. For Privacy Act requests and appeals, individuals may verify their identity by providing (1) adequate identification, which includes one of the following: a copy of a government-issued identification card, driver's license, Medicare card, birth certificate, or passport; and (2) a signed and dated statement that is either notarized or submitted under 28 U.S.C. 1746. Individuals may provide their SSN as part of a Privacy Act request or appeal; however, individuals are not required to provide their SSNs to submit a FOIA or Privacy Act request or appeal. The USITC does not request SSNs for either purpose.

The identity verification statement must include the following information:

- A declaration that your statement is true and correct under the penalty of perjury (18 U.S.C. 1001), and that you are the person named in your Privacy Act request; and
- An acknowledgement that you understand the criminal penalty in the Privacy Act for requesting or obtaining any record(s) under false pretenses

Privacy Act requestors will need to provide proof of identification prior to any release of records. An individual requesting records from the USITC through the FOIA or Privacy Act processes may need to create an account on the USITC website, thus creating logon credentials. To create an online account to submit a FOIA request via the

ArkCase service, individuals will need to establish logon credentials, including information such as a username and password. By creating this account, an individual can receive records from the USITC.

Documents in the FOIA system may contain SSNs. The USITC redacts this information before providing documents to requestors.

USITC staff accounts in the ArkCase system contain information such as name, username, network login credentials, and email address. Documents requested through FOIA may include personnel information on USITC staff, such as employment history or other personnel records for staff whose information is subject to FOIA requests. The USITC redacts personal information such as personal contact information, home address, and SSN before providing documents to requestors. Staff in OSE, the Office of the General Counsel (OGC), and the Office of the Chief Information Officer (OCIO) who are assigned to work on FOIA requests can access this information.

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

The FOIA and Privacy Act request and appeals processes collect PII, including contact information, from members of the public and USITC staff. Any member of the public may submit a FOIA or Privacy Act request or appeal. Depending on the nature of a FOIA request, individuals may also need to submit a payment to access the information that they request. Both systems collect PII on USITC staff who administer these processes.

As part of the FOIA and Privacy Act request and appeals processes, the USITC, through the ArkCase system and in files stored outside of that system, collects, uses, maintains, and disseminates the PII of members of the public who submit FOIA or Privacy Act requests and appeals and of USITC staff who process those requests. In addition, records that are responsive to FOIA and Privacy Act requests and appeals that the USITC stores in the ArkCase system or in files outside of that system may contain PII about parties to Commission investigations (e.g., party representatives, legal counsel, expert witnesses), members of the public, and USITC staff.

2.3 Who owns and/or controls the PII?

The USITC. Armedia LLC owns the ArkCase system, which the USITC has a license to use. The USITC controls the FOIA and PA processes and all PII that is (1) submitted to the USITC for those processes, whether through ArkCase or other means, or (2) contained within records that the USITC determines to be responsive to a FOIA or PA request.

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.

The FOIA, as amended, 5 U.S.C. § 552, and the Privacy Act, as amended, 5 U.S.C. § 552a, authorize the USITC to collect information for FOIA and Privacy Act requests and appeals, respectively. In addition, the Federal Records Act, 44 U.S.C. § 3301 et seq., requires the USITC to make and preserve records to adequately document USITC business. The USITC's implementing regulations for the FOIA, 19 C.F.R. Part 201 Subpart C, and the Privacy Act,

19 C.F.R. Part 201 Subpart D, govern the process by which the USITC handles FOIA and Privacy Act requests and appeals, including how the USITC collects information from individuals who submit requests and appeals.

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 USITC may allow the option for individuals outside of USITC (i.e., other than USITC staff) to create accounts to access information related to FOIA or Privacy Act requests and appeals. In such instances, creating an account would involve creation of authentication information such as username, password, or authentication codes. No new information is created for USITC staff who have user accounts to access the FOIA and Privacy Act system and records. Their access to the system is granted based on their current USITC credentials.

2.6 Given the amount, type, and purpose of the information collected, discuss what privacy risks were identified and how they will be 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 mission or a business function.

The USITC uses information submitted through a FOIA or Privacy Act request or appeal, including PII, to determine whether the USITC maintains the requested information in its records, to assess whether it may legally provide the information to the requestor, and, if applicable, to release (i.e., to transmit) the relevant information to the requestor. When processing FOIA requests, the USITC stores records that are potentially responsive to FOIA and Privacy Act requests in the ArkCase service and uses the information within those records, including PII, to determine whether a record is responsive to a request or appeal and can be released to a requester. To the extent permitted by law, the USITC redacts PII before releasing records to requesters.

FOIA and Privacy Act request files, including files within the ArkCase service, may include PII of USITC staff. For example, FOIA and Privacy Act processing records often include communications between the USITC and the requester (e.g., emails, disposition letters), which contain USITC staff names, phone numbers, and email addresses. They also often include internal notes and internal communications about a request. The USITC uses this information to track internal processing of a request, to communicate with requesters, and to respond to FOIA and Privacy Act requests.

The USITC also uses PII that requesters submit as part of FOIA and Privacy Act requests to generate internal and external logs of requests. The USITC uses these logs to track and report out on the requests that it receives. To the extent permitted by law, the USITC redacts PII from logs of FOIA and Privacy Act requests before publishing or releasing those logs publicly.

The ArkCase service has an audit report functionality that is accessible only to authorized USITC staff and provides information on actions taken in the system. The audit reports include the name of the user (e.g., requester or USITC staff member) who initiated an action in the system for a request. The USITC uses this information to record USITC actions on a FOIA or Privacy Act request, track the status of requests, and troubleshoot any processing issues with a request. ArkCase staff with a need-to-know have access to provide support functionality to USITC and may have access to records in the system containing PII in order to troubleshoot issues and provide technical support to USITC.

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 individuals who submit FOIA or Privacy Act requests and appeals to verify the accuracy of their information when they submit a request or appeal. However, USITC staff may uncover, or requesters may report, inaccuracies in the information associated with a FOIA or Privacy Act request or appeal while the USITC is processing it. USITC staff also confirm the accuracy of PII collected for Privacy Act requests and appeals when verifying the identity of the requester. USITC staff can correct inaccurate or erroneous information or data, as necessary, at any point during these processes.

OCIO creates USITC ArkCase accounts and administers access to the service for USITC staff who need access as part of their job duties. OCIO creates USITC staff accounts using USITC system information. USITC staff are responsible for verifying the accuracy of PII associated with their ArkCase user accounts and their activity on ArkCase. USITC staff can contact OCIO to report any issues with their accounts.

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

When an individual submits a FOIA or Privacy Act request or appeal with the USITC, the FOIA and Privacy Act submission forms on the USITC website indicate the required and optional data fields. The USITC only collects data that can be used to identify the requestors and to contact them, as necessary, in response to their requests (e.g., name, email address, telephone number, office address).

USITC staff accounts in ArkCase 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)?

Records related to contact information of FOIA and Privacy Act requestors and other information related to FOIA or Privacy Act requests are covered by the following items in NARA General Records Schedule 4.2: Information Access and Protection Records:

- Item 020: Access and disclosure request files;
- Item 040: Records of accounting for and controlling access to records requested under FOIA, PA, and Mandatory Declassification Review (MDR);
- Item 050: Privacy Act accounting of disclosure files;
- Item 065: Privacy complaint files; and
- Item 090: Privacy Act amendment request files.

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

The USITC destroys hard copies of files related to FOIA and Privacy Act requests and appeals and electronically deletes electronic files related to these processes.

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

Yes. OSE can conduct searches using PII of a requestor or USITC staff (e.g., names and contact information) to retrieve information within FOIA or Privacy Act records. OSE also creates user access (i.e., audit) reports, which query and pull PII. The administrator role in ArkCase can view audit features in the system (e.g., identifying user actions). USITC staff with system accounts who do not have administrator roles can review certain audit records (e.g., records of actions taken in response to FOIA or Privacy Act requests).

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)?

ITC-20: Freedom of Information Act and Privacy Act Records.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

OSE is the primary user of information collected via the FOIA and Privacy Act request and appeals processes, though it shares such information with other agency offices, as needed, to process these requests and appeals. For instance, OSE may share information with the Office of Human Resources (HR) for FOIA or Privacy Act requests or appeals related to personnel records. Additionally, other stakeholder offices with records relevant to the FOIA or Privacy Act request(s) may provide, by internal email or internal secure file transfer on the USITC shared storage drive, relevant records containing PII.

OSE shares all FOIA and Privacy Act requests and appeals with OGC. OGC provides legal advice for FOIA and Privacy Act requests and appeals.

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

OSE shares the names and contact information of FOIA or Privacy Act requestors with specific individuals within USITC offices on a need-to-know basis as necessary for those individuals to process requests and appeals.

OSE provides all information for FOIA and Privacy Act requests and appeals, including relevant responsive or non-responsive records, to attorneys in OGC, as needed, for OGC to provide legal advice and review.

4.3 How is the information transmitted or disclosed?

Information is shared via email and/or secure internal file sharing functions. OSE uses ArkCase to share information within OSE and to provide FOIA request and appeal files to OGC for OGC review. OSE and OGC will review documents and redact information as needed. The USITC provides documents to requestors through the ArkCase portal or via email.

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 system.

5 EXTERNAL SHARING AND DISCLOSURE

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

The USITC shares request and appeal information with other federal agencies when it must consult with them regarding a FOIA request or appeal. In addition, the USITC, when requested, releases FOIA logs that provide the names of requesters. However, the USITC does not share PII of individuals submitting FOIA or Privacy Act requests or appeals with external entities, unless specifically requested by a consulting agency or as required by law.

ArkCase allows anyone to access a report of FOIA requests and appeals, and the USITC releases records in this system to FOIA requesters.

Armedia staff have access to FOIA and Privacy Act data as part of data migration tasks, but access is limited to staff with job duties that require access to this data and a need-to-know.

5.2 What information is shared and for what purpose?

The USITC shares request and appeal information with other federal agencies when it must consult with them regarding a FOIA request or appeal. In addition, the USITC, when requested, releases FOIA logs that provide the names of requesters. However, the USITC does not share contact information of individuals submitting FOIA or Privacy Act requests or appeals with external entities.

ArkCase allows anyone to access a report of FOIA requests and appeals, and the USITC releases records in this system to FOIA requesters.

Armedia staff have access to FOIA and Privacy Act data as part of data migration tasks, but access is limited to staff with a need-to-know and job duties that require access to this data.

5.3 How is the information transmitted or disclosed?

The USITC typically provides information regarding FOIA or Privacy Act requests and appeals to external entities via email. The USITC limits the PII in these transmissions to the minimum necessary. The USITC does not share PII of individuals submitting FOIA or Privacy Act requests or appeals with external entities, unless specifically requested by a consulting agency or as required by law.

5.4 Are there any agreements with external entities concerning the security and privacy of information once it is shared, such as a Memorandum of Understanding (MOU)?

Not applicable. The USITC does not share PII of individuals submitting FOIA or Privacy Act requests and appeals with external entities, unless specifically requested by a consulting agency or as required by law.

The USITC does not have agreements with external entities regarding the sharing of information pursuant to the FOIA and the Privacy Act. Other federal agencies that receive information from the USITC for purposes of consultation on a FOIA or Privacy Act request or appeal are subject to all relevant legal requirements concerning the security and privacy information as applied to federal agencies.

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

The USITC does not share PII of individuals submitting FOIA or Privacy Act requests and appeals with external entities, unless specifically requested by a consulting agency or as required by law. As noted previously, Armedia staff have access to FOIA data as part of data migration tasks. Access is limited to staff with job duties that require access to this data and have a need-to-know. These Armedia staff are required to sign non-disclosure agreements (NDAs) that describe requirements for protecting Privacy Act data.

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

Not applicable. The USITC does not share PII of individuals submitting FOIA or Privacy Act requests and appeals with external entities, unless specifically requested by a consulting agency or as required by law. Employees of other federal agencies are required to complete annual FOIA and privacy training in accordance with legal requirements.

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

The USITC does not share PII of individuals submitting FOIA or Privacy Act requests and appeals with external entities, unless specifically requested by a consulting agency or as required by law. As noted, contractors are required to sign NDAs regarding their access to and use of data collected as part of the FOIA and Privacy Act processes.

ArkCase provides a functionality for USITC to view audit records of user actions such as viewing, reading, downloading, and editing documents within the system. These functions allow USITC to audit user access to data, including access by any Armedia users.

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 PII of individuals submitting FOIA or Privacy Act requests and appeals with external entities, unless specifically requested by a consulting agency or as required by law.

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) that discusses the USITC's privacy practices and the types of information that the USITC collects. The privacy page also includes a link to the USITC's PIAs and SORNs.

In addition, the USITC website provides the public with guidance, information, and the rules regarding the FOIA process (https://www.usitc.gov/offices/secretary/foia/index.htm).

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

Yes. Submitting a FOIA or Privacy Act request or appeal is voluntary; thus, individuals are not required to share their information with the USITC. However, the USITC may be unable to process a FOIA or Privacy Act request or appeal without receiving required information, as indicated, from requestors.

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 submitting a FOIA or Privacy Act request or appeal, potential users may read the website privacy policy (located at www.usitc.gov/privacy), the applicable SORN (ITC-20, Freedom of Information Act and Privacy Act Records), or this PIA to understand how information collected through these processes is used. If they object to how the data is used, they are not required to submit a FOIA or Privacy Act request or appeal, and thus they would not consent to the use of their data by USITC.

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 through the FOIA and Privacy Act processes and how this information is used. This risk is mitigated through the publication of this PIA on the USITC website, the publication of the relevant SORN, ITC-20, and by including a link to the USITC Privacy Policy on USITC web page.

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?

Members of the public may request corrections or amendments to inaccurate PII by contacting OSE directly or by submitting a Privacy Act request in accordance with the USITC Privacy Act Rules. USITC staff whose information is incorrect may contact the USITC Office of Chief Information Officer (OCIO) to update their information.

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

This PIA and SORN ITC-20 provide notice to individuals regarding access and amendment procedures.

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

Not applicable. Individuals may amend their information through the process outlined in this document.

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.

Individuals may contact OSE or submit a Privacy Act Request in accordance with the USITC Privacy Act Rules to contest the accuracy of their information in the system.

8 TECHNICAL ACCESS AND SECURITY

8.1 Who has access to the PII in the system?

Authorized USITC staff in OSE and OGC will have access to the PII of all individuals who submit FOIA and Privacy Act requests and appeals to process and respond to those requests and appeals. OSE and OGC staff will also have access to the PII in records that they review in response to a FOIA or Privacy Act request or appeal. In addition, USITC staff in other offices will have access to requester PII and PII in responsive records on a need-to-know basis to process FOIA and Privacy Act requests and appeals.

Authorized information system administrators in OSE and OCIO will have access to user account information to conduct audits of user activity and to perform other system administration tasks (e.g., updating the website and software, disabling inactive accounts), as necessary.

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

USITC users who access these systems are assigned role-based privileges based on need-to-know and their job responsibilities (for USITC staff). In addition, USITC information system administrators, which includes staff in OSE and OCIO, are granted access to the systems to conduct audits of user activity and to perform system administration tasks, as necessary.

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

Users are granted access to FOIA and Privacy Act records on a need-to-know basis, as determined by OSE.

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

Internal USITC users are granted access to information in the FOIA and Privacy Act records on a need-to-know basis and are granted the least privilege needed to conduct their duties. The USITC implements auditing controls in accordance with the NIST SP 800-53 guidance to track user behavior and identify misuse of the system. The ArkCase software has auditing capability to track actions conducted by users in the system.

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

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

FOIA and Privacy Act records are stored on the USITC network (ITCNET), which 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.