Miscellaneous Tariff Bill Petition System (MTBPS) Privacy Impact Assessment (PIA)

5/14/2019

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).

Miscellaneous Tariff Bill Petition System (MTBPS) Privacy Impact Assessment (PIA)

USITC PRIVACY PROGRAM

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 the 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 Miscellaneous Tariff Bill Petition System (MTBPS) was developed pursuant to the American Manufacturing Competitiveness Act of 2016 (Public Law 114-159). MTBPS facilitates the electronic submission of petitions and comments from members of the public requesting temporary duty suspensions and reductions on certain imported goods. MTBPS also supports USITC staff analysis of those petitions and comments. Based on information within the system, MTBPS generates preliminary and final reports on the miscellaneous tariff bill petitions submitted. The American Manufacturing Competitiveness Act of 2016 requires the USITC to deliver these preliminary and final reports to certain Congressional committees in a specified timeframe.

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: MTBPS requires users to log-in with a username and password to view and/or submit petitions and/or comments. In creating an account, users must provide their first and last names, contact phone numbers, and email addresses. Most users provide their work contact information, but some may submit personal contact information. When submitting a petition or comment, the submitter is asked to provide the petitioning or commenting company name and address as well as the first and last name of a contact at the company and their email address and phone number. If the submitter is an independent representative filing on behalf of the company (e.g., outside counsel), the system separately asks for the independent representative's first and last name, firm name, email address, and phone number.

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

MTBPS collects information from people who use the system to view or submit petitions or comments, as well as from people whom USITC staff or Department of Commerce staff have contacted or wish to contact because they have knowledge about petition(s) or comment(s). These people may include USITC employees, contractors, employees from other government agencies, congressional staff, executive branch staff, and members of the public. The majority of system users and contacts are employees of companies, trade associations, or law firms seeking to obtain or comment on the duty suspensions and reductions provided for by the MTB process.

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.

The American Manufacturing Competitiveness Act of 2016, Public Law 114-159, enacted May 20, 2016, requires the USITC to collect petitions and comments from members of the public. Section 3(b)(2)(A) specifically indicates that the USITC must collect the name and address of petitioner. Pursuant to the Paperwork Reduction Act, the USITC received clearance from OMB to collect petition and comment information (OMB No. 3117-0228) for the first cycle of MTB petitions mandated by the Act. This clearance expires September 30, 2019. The process for obtaining clearance from OMB for the second cycle of petitions began with the publication of a Federal Register notice on April 4, 2019.

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 MTBPS 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.

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 business function.

USITC staff use this information if they have procedural or substantive questions about a petition or comment and must contact someone with knowledge of the petition/comment and the petitioned for or commented on product.

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

MTBPS relies on users to verify the accuracy of their data before the user creates a new account to access the system and/or submitting a petition or comment. Users may contact mtbpshelp@usitc.gov to fix errors in their account information.

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

MTBPS only requires information needed to sufficiently identify and contact a user in the event there is a question about their account, petition, and/or comment. In addition, the USITC receives authorization to collect petition and comment information from OMB pursuant to the Paperwork Reduction Act (PRA) for each MTB cycle. The PRA requires that agency information collections minimize duplication and burden on the public, have practical utility, and support the proper performance of the agency's mission.

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)?

Temporary. Delete/destroy when 20 years old. General Records Schedule 3.2, Information Systems Security Records, applies to these records.

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

Hard copy files are destroyed. There is not currently a mechanism to archive electronic data or files. However, no records are due to be destroyed or deleted in accordance with the disposition schedule, as data and files created in MTBPS only date to October 14, 2016. If necessary, USITC will update MTBPS to dispose of records in accordance with the disposition schedule.

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

The MTBPS cannot be searched or records retrieved by any PII unless an individual provides a first and last name in the petitioning or commenting company name field. The system can be searched by querying the petitioning and commenting company name field. If an individual would put their name in one of those fields, it would be

searchable on both the internal and external interface. However, it is not the USITC's practice to search MTBPS by an individual's name.

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)?

N/A.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

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

MTBPS information is accessed by staff from the Office of the Chief Information Officer, Office of the Secretary, Office of Industries, Office of Tariff Affairs and Trade Agreements, Office of the Commissioners, Office of the General Counsel, and Office of Analysis and Research Services. A limited number of employees in other USITC offices, if they are assigned to work on MTB petitions, may have access as well.

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

The Office of the Chief Information Officer accesses user account records to manage user account privileges and audit user activity. Petition and comment submissions, including the contact information provided as part of the petition and/or comment, are made available to the USITC program offices in order to contact the petitioner or commenter should there be questions regarding the petition or comment.

4.3 How is the information transmitted or disclosed?

The information is shared via the internal MTBPS user interface.

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. 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.

5 EXTERNAL SHARING AND DISCLOSURE

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

In addition to what is provided via the MTBPS external application, USITC staff shares the information in a delimited, text file with the Department of Commerce and U.S. Customs and Border Protection.

5.2 What information is shared and for what purpose?

All information collected as part of the petitions and comments, including data marked as business confidential and PII, is shared with the Department of Commerce (DOC) and U.S. Customs and Border Protection (CBP) for purposes of the report those agencies must prepare in accordance with Section 3(c) of the American Manufacturing Competitiveness Act of 2016. The DOC contacts people with knowledge about petition(s) or comment(s) and may share their contact information (e.g., company name, individual contact name, phone number) with USITC staff for the purpose of the reports the USITC must prepare in accordance with Sections 3(b)(3)(C) and (E) of the American Manufacturing Competitiveness Act of 2016.

5.3 How is the information transmitted or disclosed?

The information is transmitted exclusively via a secure web-based portal.

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)?

The USITC signed two MOUs, one with the (DOC), signed November 18, 2016, and one with CBP, signed January 26, 2017.

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

Yes. All contract staff are bound by contract language stating they will not disclose sensitive information, including PII, and are required to sign nondisclosure agreements. In addition, the contract language states that contract staff must complete required agency training regarding privacy and information security.

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

The USITC does not provide staff at the DOC or CBP with training on how to use data related to MTB petitions and comments. The MOUs referenced in question 5.4 state that employees, interns, or qualified contractors of the respective agencies who are afforded access to information shared under the MOU have a qualified background investigation completed in accordance with applicable agency standards based on the type of information they are accessing.

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

No.

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

USITC staff, in collaboration with MTB management at the DOC and CBP, concluded that a web-based portal was the most secure way to transmit MTB-related information. Access to the information shared via the portal is restricted to a limited number of staff at the USITC, DOC, and CBP in order to mitigate the risk of unauthorized disclosure.

6 NOTICE

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

The MTBPS website links to a page on privacy (https://www.usitc.gov/privacy) which discusses the USITC's privacy practices and the types of information the USITC website collects. The privacy page will also include a link to the MTBPS PIA.

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

Individuals are not required to provide their information to MTBPS. However, if they do not provide the necessary information, they will be unable to create a user account, login to the system, or submit or view a petition/comment.

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 MTBPS account, potential users may read the MTBPS Terms of Use Agreement to understand how MTBPS account information is used. If they object to how the data is used, they are not required to create an MTBPS account, and thus would not consent to the use of their data by MTBPS.

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 MTBPS 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 MTBPS homepage.

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?

MTBPS users may access their information by logging in to the MTBPS website and may request updates to their information by contacting mtbpshelp@usitc.gov.

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

The MTBPS website contains a link to the MTB Handbook on Filing Procedures, which provides instructions for creating and updating account information, as well as instruction for filing petitions and comments. The MTBPS homepage also contains a link to mtbpshelp@usitc.gov, which users can contact to update account information.

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

Not applicable. Users may update their account information by contacting mtbpshelp@usitc.gov.

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.

Should users need to update their user account information or the information provided as part of a petition or comment, they can contact mtbpshelp@usitc.gov. 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?

MTBPS user account information is accessible only by Office of Chief Information Officer staff authorized to conduct account administration tasks (e.g., creating an account, modifying account information, etc.) for system maintenance purposes. All MTBPS users can access incidental PII that appears in publicly available petition and comment submissions. This incidental PII may take the form of petitioner or commenter contact information included in the letterhead or text of a file uploaded with a petition or comment submission in MTBPS.

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 MTBPS to perform system administration tasks (e.g. updating the website and software).

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

Users are assigned roles based on their job title and function. A log is maintained by the MTB program manager outlining the USITC staff who have access to the internal system.

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 MTBPS on a need-to-know basis and are granted the least privilege needed to conduct their duties. MTBPS 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?

MTBPS 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)?

MTBPS has a current ATO as sub-system of the USITC's ITCNET system 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 MTBPS to address security controls that are not implemented or operating effectively.