U.S. International Trade Commission

Electronic Document Information System

Privacy Impact Assessment

March 10, 2010

Final

TABLE OF CONTENTS

Document Change History

Version Number	*Date*	*Description*
0.1	06/01/08	Draft Version
1.0	07/22/08	Final Version
1.1	03/20/2009	EDIS Collaboration Draft
1.2	03/25/2009	Collaboration Draft Incorporating Comments from The Offices of General Counsel, The Secretary and Docket Services
1.3	04/03/2009	Editorial Clean-up
1.4	07/10/2009	Final PDF
2.0	02/19/2010	Draft to update the required authentication by the Public (3.3.1)
2.1	03/01/2010	Collaboration Draft Incorporating Comments from the Offices of the Secretary, CIO and Docket Services Division.
2.2	03/09/2010	Updated with comments from the Office of General Counsel

1. Preface

Under the E-Government Act of 2002 and Office of Management and Budget (OMB) Memorandum 03-22, all agencies must conduct a privacy impact assessment (PIA) before developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate information in identifiable form (IIF) from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of IIF for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). A PIA is an analysis designed to:

- Ensure that information handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining, and disseminating IIF in an electronic information system; and
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

In accordance with the guidance set forth in OMB Memorandum 03-22, which identifies the major triggers for conducting PIAs, the United States International Trade Commission (USITC or Commission) completed a PIA to reflect the current system.

1.1 Methodology

The methodology for this PIA will establish the compliance of the Electronic Document Information System (EDIS) with privacy legislation, regulations, guidance, and best practices. Figure 1 lists the Federal legislation.

Figure 1

	Federal Legislation
Privacy Act of 1974	‣ establishes "Fair Information Practices" for the collection, maintenance, and use of personal information by federal agencies
E-Government Act of 2002	‣ requires federal agencies to complete a Privacy Impact Assessment for each new information system and for existing systems as major changes are made ‣ outlines required content of PIAs ‣ directs the OMB Director to issue further guidance ‣ requires the Department's Chief Information Officer (CIO) to review and, if possible, publish the results of the PIA ‣ components of the *E-Government Act* include FISMA and Section 208, the Privacy Provisions
Children's Online Privacy Protection Act of 1998 (COPPA)	‣ applies to all Web sites that collect personal information from children under 13 ‣ affects content of privacy policy ‣ specifies when and how to seek verifiable consent from a parent ‣ lists operators' responsibilities to protect children's privacy and safety online
Clinger-Cohen Act of 1996 (formerly the *Information Technology Management Reform Act*)	‣ intends to improve the productivity, efficiency, and effectiveness of federal programs through the improved acquisition, use, and disposal of IT resources ‣ places the burden of incorporating privacy controls into IT investments at the agency and CIO levels
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	‣ affects healthcare providers, health plans, and health care clearinghouses, including federal agencies and institutions ‣ ensures that administrative simplification provisions include privacy protections, which were detailed in corresponsing federal regulations
Paperwork Reduction Act of 1995 (PRA)	‣ increases the efficiency of the federal government's information collection practices ‣ makes senior information resources managers, such as CIOs, responsible for overseeing the information collection process and paperwork reduction ‣ is responsible for creating the Office of Information and Regulatory Affairs within OMB to provide central oversight of information management activities across the federal government
Computer Matching and Privacy Protection Act of 1988	‣ affects how federal agencies may share data with other federal and state agencies ‣ adds procedural requirements for agencies, including the requirements that agencies give notice to and obtain consent from individuals whose data will be matched ‣ implements regulations to identify PIAs as a federal best practice
Freedom of Information Act of 1966 (FOIA)	‣ applies to all agencies of the executive branch ‣ requires agencies to release information held by those agencies to individuals requesting it in writing, unless one of nine exceptions applies

1.2 Requirements

Conducting a PIA provides an opportunity to identify privacy vulnerabilities and risks associated with information systems. Once risks and vulnerabilities are identified, system managers can identify strategies and controls to mitigate them. Formal PIAs provide a number of advantages over ad hoc evaluations. These advantages include:

- Producing a PIA Summary suitable for meeting the supporting documentation requirements for budget and funding documents (i.e., OMB exhibit 300s and exhibit 53s)[1];
- Providing inputs for required reporting documents (e.g., Plan of Action and Milestones [POA&M]);
- Providing a reliable basis for policy and system design decision-making and system design;
- Generating and improving public confidence by anticipating and addressing privacy concerns; and
- Improving the understanding of potential privacy risks, exposures, and liabilities.

1.3 Document Organization

The document is organized into the following sections:

- System and data characterization;
- Information sharing practices;
- Appendix A: Privacy Analysis Worksheet; and
- Appendix B: Glossary

2. System and Data Characterization

EDIS is one of the USITC's major applications and is a complex document management system which automates the processes for managing documents related to the USITC's investigatory roles. EDIS supports the Commission's investigative processes and the functions of the Offices of The Secretary to the Commission, Docket Services, Investigations, General Counsel, Unfair Import Investigations, Administrative Law Judges and others. Both Commission users and external users will see improvements in overall performance, usability, and reliability over the previous version of EDIS. The Commission will achieve these improvements through (1) a central home page for all EDIS functions, (2) instant user notification for validation of document submissions, (3) improvements in the electronic submission interface, (4) improved internal functionality, and (5) the implementation of new hardware architecture featuring system redundancy. The system also provides enhanced security features to allow extended access to sensitive documents with continued confidentiality protections. Sensitive documents are only available to Commission users who consist of authorized employees, contractors, interns and volunteers.

[1] USITC does not prepare Exhibit 300s and 53s, because the Commission presents its budget directly to The Congress.

EDIS's architecture is comprised of various components that are incorporated into the existing USITC network infrastructure. The hardware that supports EDIS includes servers, workstations, scanners, and storage devices. EDIS production, development and test environments are located at USITC in Washington, DC. All EDIS users will access the application via a web browser.

EDIS contains IIF. EDIS and Docket Services Division personnel perform a general review of the information contained in the documents submitted to the system. Following is a list of common data elements:

- Name
- Company
- Position title
- Address
- Email address
- Phone number
- Legal documents (non-criminal)
- Office location
- Investigation # (assigned by the USITC)

3. Information Sharing Practices

EDIS is not connected to any external system and is hosted on the USITC network infrastructure. All documents within EDIS are submitted to the system by registered users. The Office of the Secretary maintains a database which is used to track information which is entered into EDIS. This information includes Investigation Number and Administrative Protective Order (APO) service list. The documents within EDIS can originate from a number of federal and private sources. Documents from Congress and Federal agencies such as the Office of the U.S. Trade Representative and the Department of Commerce are regularly entered into EDIS.. Additional sources of EDIS documents include law firms and any citizen (for example, a small business owner) who may have an interest in any USITC investigation.

All documents entered into EDIS must have a security rating, which is assigned by the submitting party. The Docket Services staff verify this security rating based on filer information. The Docket Services Division performs additional assessments to ensure potential errors are identified and addressed. The purpose of the security rating is to determine the appropriate level of user access to the document. Security ratings of documents are as follows:

- **Administrative-** contains records management documents. Access is restricted to OSE (Office of the Secretary) and Docket Services staff
- **Confidential**-contains Business Proprietary Information (BPI) or Confidential Business Information (CBI). Access is only permitted for internal USITC users. To users at this level, access has been approved by the Office of the Secretary.
- **Limited-** Public transcripts of USITC proceedings which are withheld from public access for a 60 day period following the court activity. All internal USITC staff have access to this level of documents.
- **Public**- all documents which are accessible by the general public.
- **Privileged** – documents of a sensitive nature with limited user access.

The USITC Docket Services Division is responsible for accepting electronically submitted files into EDIS and scanning the paper copies to be loaded into EDIS. Personnel from the Docket

Services Division have the ability to review documents and edit/alter files for EDIS. These edit permissions only allow the ability to re-align documents and check for page length consistency (for example, if the document was listed as 40 pages long, Docket Services will check for 40 pages). If one of the two types of errors are detected the Docket Services personnel will rescan the document.

There are two main types of EDIS users – internal and external. All internal EDIS users can access all public and limited documents. Permission to view documents with security rating above public are only granted for up to a specified security level based on office affiliation and need-to-know access rights of that office. External EDIS users can only access public documents. Internal users of EDIS are required, at minimum, to have a National Agency Check and Inquiries (NACI) background investigation. Any contractors operating on the system must have a background Suitability check as is required of all non-national security information systems. This investigation examines whether the user is suitable to operate with the permissions of a Federal employee.

EDIS external users have access to the following:

- Filing - Cover Sheet
- Filing - e-Filing
- Reports - Document Filing
- Search - Advanced
- Search - Conf Metadata
- Search - Investigation
- Search - Limited Metadata
- Search - Public Documents
- Search - Public Metadata
- Search - Validated
- User - Change Password
- User - Change Sec. Questions
- Reports App Access
- User - Profile Edit
- General - Contact us
- General - Forgot Password
- General - Login
- General - Logout
- General - Registration
- General - Welcome
- General - What's New
- Help - Doc List (Pub)

There is a Remote Subscriber Service (RSS) feed which users may access. External users can receive RSS notification for document approval.

Appendix A: Privacy Analysis Worksheet

The PIA determines what kind of IIF is contained within a system, what is done with that information, and how that information is protected. Systems with IIF are subject to an extensive list of requirements based on privacy laws, regulations, and guidance.

System Name	Electronic Document Information System (EDIS)
Agency	U.S. International Trade Commission
System Location	500 E Street, SW Washington, DC 20436
System Point of Contact (POC)	Joel Moeller Title: E-Business Division Manager Phone Number: 202-205-3347 E-Mail: EDIS3Help@usitc.gov
Activity/Purpose of System:	EDIS is a document management system which automates the processes for managing documents related to USITC's investigatory role. The EDIS electronic repository is the official record of legal filings with the USITC. The documents may be retrieved, viewed and printed, by authorized persons, via a World Wide Web interface.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
	System Characterization and Data Categorization				
1	**Does/Will the United States International Trade Commission own the system?** Note: If no, identify the system owner in the Comments column.	☒	☐	☐	
2	**Does/Will the United States International Trade Commission operate the system?** Note: If no, identify the system operator in the Comments column.	☒	☐	☐	
3	**Identify in the Comments column the life-cycle phase of this system.**				☐ Initiation ☐ Develop/Acquisition ☐ Implementation ☒ Operations/Maintenance
4	**Has/Have any of the significant changes listed in the Comments column occurred to the system since the conduct of the last PIA?** **If yes, please check which change(s) have occurred.**	☒	☐	☐	☐ Conversions ☒ Anonymous to Non-Anonymous ☐ Significant System Management Changes ☐ Significant Merging ☐ New Public Access ☐ Commercial Sources ☐ Internal Flow or Collection ☐ New Interagency Use ☐ Alteration in Character of Data
5	**Is the system (or will the system be) a stand-alone system or a networked system?**				☐ Stand-alone ☒ Networked ☐ Other (Please explain)
6	**Is the system (or will the system be) a sensitive system?**	☒	☐	☐	
7	**Is the system (or will the system be) a General Support System (GSS) or a Major Application (MA)?** Note: If yes, identify in the Comments column whether the system is a GSS, MA, or sensitive system.	☒	☐	☐	☐ General Support System (GSS) ☒ Major Application (MA) ☐ Other (Please explain)

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
8	**Does/Will the system *contain* information in identifiable form (IIF) within any database(s), record(s), file(s) or website(s) hosted by this system?** Note: If yes, check all that apply in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category. Please note: This question seeks to identify all personal information contained within the system. This includes any IIF, whether or not it is subject to the *Privacy Act*, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the system contains <u>no</u> IIF, none of the remaining questions in this section and the information sharing practices section apply. Please mark the remaining questions with an N/A and proceed to the Website practices section at question 30.	☒	☐	☐	**Personal Information:** ☒ Name ☐ Date of birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name ☐ Vehicle identifiers (e.g., license plates) ☒ Mailing address ☒ Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☒ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) ☒ E-mail address ☐ Education records ☐ Military status and/or records ☒ Employment status and/or records (firm that user is employed by) ☒ Foreign activities and/or interests ☐ Other: System ID (combination of USITC and last name) ☒ Other: User name/ID ☒ Other: Office location

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
					Comment: There is no limit to the type of information and data elements contained in the system. On the most basic level, almost all documents contain the name of an individual representing/participating in a USITC investigation. Beyond that, it is possible that a document may contain any of the above listed data IIF.
9	**Indicate the categories of individuals about whom IIF is or will be collected.**				☒ Employees (an EDIS document could possibly include the name of the USITC employee acting on the investigation) ☒ Public citizens ☐ Patients ☒ Business partners/contacts (federal, state, local agencies) ☒ Vendors/Suppliers/Contractors

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
10	**Are records on the system (or will records on the system be) retrieved by one or more data elements?** Note: If yes, specify in the Comments column what method is or will be used in retrieving the records (i.e., using a record number, name, social security number, or other data element or record locator methodology). If the category of personal information is not listed, please check "Other" and identify the category.	☒	☐	☐	**Personal Information:** ☒ Name ☐ Date of birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name ☐ Vehicle identifiers (e.g., license plates) ☐ Mailing address ☐ Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☒ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) ☒ E-mail address ☐ Education records ☐ Military status and/or records ☒ Employment status and/or records (firm that user is employed by) ☒ Foreign activities and/or interests ☐ Other: System ID (combination of USITC and last name) ☒ Other: Office location ☒ Other: User name/ID ☐ Other: Password

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
					Comment: A document can be queried by any of the above noted data items or any key word entered by a user.
11	**Are/Will 10 or more records containing IIF [be] maintained, stored or transmitted/passed through this system?**	☒	☐	☐	
12	**Is the system (or will it be) subject to the Privacy Act?** Note: If the answer to questions 8, 10, and 11 were "yes," the system will likely be subject to the *Privacy Act*. System owners should contact their Privacy Contact for assistance with this question if they are less than sure about the applicability of the *Privacy Act*.	☐	☒	☐	
13	**Has a Privacy Act System of Records (SORN) Notice been published (or will one be published) in the Federal Register?** If no, explain why not in the Comments column.	☐	☐	☒	☐ No IIF is contained in the system. ☐ IIF is in the system, but records are not retrieved by IIF. ☐ Should have published an SORN, but was unaware of the requirement. ☐ System is required to have an SORN but is not yet procured or operational. ☒ Other: On the advice of the Office of General Counsel, a SORN is not required.
Information Sharing Practices					
14	**Is the IIF in the system voluntarily submitted (or will it be)?**	☒	☐	☐	User information is required during the registration process, whether users elect to electronically file legal documents through EDIS or want to read publicly available legal documents. IIF contained in scanned documents is not regulated. It is possible that IIF on an individual may be entered without the consent/knowledge of that individual, as part of the documentation compilation and filing processes.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
15	**Does/Will the system *collect* IIF from individuals?** Note: If yes, identify in the Comments column the IIF the system collects or will collect directly from individuals. If the category of personal information is not listed, please check "Other" and identify the category.	☒	☐	☐	**Personal Information:** ☒ Name ☐ Date of birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name ☐ Vehicle identifiers (e.g., license plates) ☒ Mailing address ☒ Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☒ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) ☒ E-mail address ☐ Education records ☐ Military status and/or records ☒ Employment status and/or records (law firm that user is employed by) ☐ Foreign activities and/or interests ☒ Other: User name/ID ☒ Other: Office location

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
					Comments: EDIS does not attempt to collect IIF from individuals outside of the user registration process. The system only allows the electronic filing of legal documents. The system does not control what information is contained within these documents.
16	**Does/Will the system *collect* IIF from *other resources* (i.e., databases, Websites, etc.)?** Note: If yes, specify the resource(s) and IIF in the Comments column.	☐	☒	☐	☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____
17	**Does/Will the system *populate* data for *other resources* (i.e., do databases, Websites, or other resources rely on this system's data)?** Note: If yes, specify resource(s) for each instance in the Comments column.	☐	☒	☐	☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____ ☐ Resource: _____
18	**Does/Will the system *share* or *disclose* IIF with other agencies external to USITC, or other people or organizations outside USITC?** Note: If yes, specify with whom and for what purposes, and identify which data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	☐	☒	☐	
19	**If the IIF in the system is or will be matched against IIF in one or more other computer systems, are (or will there be) computer data matching agreement(s) in place?**	☐	☐	☒	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
20	**If data matching activities will occur, will the IIF be de-identified, aggregated, or otherwise made anonymous?** Note: If yes, please describe this use in the Comments column.	☐	☐	☒	☐ De-identified ☐ Aggregated ☐ Other
21	**Is there a process, either planned or in place, to notify organizations or systems that are dependent upon the IIF contained in this system when changes occur (i.e., revisions to IIF, when the system encounters a significant change, or is replaced)?**	☒	☐	☐	External users can receive RSS notification for document approval.
22	**Is there a process, either planned or in place, to notify and obtain consent from the individuals whose IIF is in the system when significant changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection)?**	☐	☒	☐	An updated PIA will be posted if IIF collection and use change. Consent will not be solicited as public users of EDIS voluntarily register to use the system, if they file legal documents electronically. USITC is not responsible for notifying parties whose IIF is contained within legal documents as part of the filing process.
23	**Is there/Will there be a process in place for individuals to choose how their IIF data is used?** If yes, please describe the process for allowing individuals choice in the Comments column.	☐	☒	☐	
24	**Is there/Will there be a complaint process in place for individuals who believe their IIF has been inappropriately obtained, used, or disclosed, or that the IIF is inaccurate?** Note: If yes, please describe briefly the notification process in the Comments column.	☒	☐	☐	Users will contact the Dockets Division or the Office of the Secretary to report an incident or issue.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
25	**Are there or will there be processes in place for periodic reviews of IIF contained in the system to ensure the data's integrity, availability, accuracy, and relevancy?** Note: If yes, please describe briefly the review process in the Comments column.	☒	☐	☐	External users who require access to EDIS data are required to establish accounts and are responsible for submitting accurate information. USITC will not verify the information external users submit for account registration.
26	**Are there/Will there be rules of conduct in place for access to IIF on the system?** Note: If yes, identify in the Comments column all users with access to IIF on the system and for what purposes they use the IIF.	☒	☐	☐	USITC personnel that are authorized to access EDIS must complete annual information security awareness training which includes instruction on handling IIF. USITC users are provided supplemental resources on handling IIF. There is a permissions process in place, administered by the Docket Services Division, for controlling internal access to sensitive information as well.
Web site Host – Question Sets					
27	**Does/Will the system host a Web site?** **Note: If yes, identify what type of site the system hosts in the Comments column.** If IIF is contained on the system and the system does not have a Web site, check "No" for all remaining questions in the "Web site Host Question Sets" section and answer questions starting with the "Administrative Controls" section beginning with question 41. If the system does not have IIF and the system does not host a Web site, please mark the remaining questions of this Privacy Analysis Worksheet with "No," sign, date and undertake the signature and review process.	☒	☐	☐	Type of site: ☐ Internet (https://edis.usitc.gov/edis3-external/page.svc?page=edis3Central:Home) ☐ Intranet - USITC Internal Users Only ☒ Both

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
28	**Is the Web site (or will it be) accessible by the public or other entities (i.e., federal, state, and local agencies, contractors, third-party administrators, etc.)?**	☒	☐	☐	EDIS is accessible by all public, state and local agencies and contractors. Registration is required to view the publicly-available information.
29	**Is a Web site privacy policy statement (consistent with OMB Section 208 Guidance) posted (or will it be posted) on the Web site?**	☒	☐	☐	www.usitc.gov/policies/privacy.htm
30	**Is the Web site's privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?**	☐	☒	☐	
31	**Does the Web site employ (or will it employ) persistent tracking technologies?** Note: If yes, identify types of cookies in the Comments column. If persistent tracking technologies are in place, please indicate the official who authorized the use of the persistent tracking technology.	☐	☒	☐	☐ Session Cookies ☐ Persistent Cookies ☐ Web bugs ☐ Web beacons ☐ Other (Describe): _____ Authorizing Official: _____ Authorizing Date: _____
32	**Does/Will the Web site have any information or pages directed at children under the age of 13?**	☐	☒	☐	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
33	**If there is a Web site directed at children, is information (including session cookies) collected (voluntarily or via tracking technologies)?** Note: If yes, identify in the Comments column any information collected, if there is a unique privacy policy for the site, and the process for obtaining parental consent if any information is collected.	☐	☐	☒	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
34	**Does/Will the Web site *collect* IIF from individuals?** Note: If yes, identify what IIF the system collects in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	☒	☐	☐	**Personal Information:** ☒ Name ☐ Date of birth ☐ Social Security Number (or other number originated by a government that specifically identifies an individual) ☐ Photographic identifiers (e.g., photograph image, x-rays, and video) ☐ Driver's license ☐ Biometric identifiers (e.g., fingerprint and voiceprint) ☐ Mother's maiden name ☐ Vehicle identifiers (e.g., license plates) ☒ Mailing address ☒ Phone numbers (e.g., phone, fax, and cell) ☐ Medical records numbers ☐ Medical notes ☐ Financial account information and/or numbers (e.g., checking account number and Personal Identification Numbers [PIN]) ☐ Certificates (e.g., birth, death, and marriage) ☒ Legal documents or notes (e.g., divorce decree, criminal records, or other) ☐ Device identifiers (e.g., pacemaker, hearing aid, or other) ☐ Web Uniform Resource Locators (URL) ☒ E-mail address ☐ Education records ☐ Military status and/or records ☒ Employment status (firm that user is employed by) ☐ Foreign activities and/or interests ☒ Other: User name/ID ☒ Other: Office location

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
					Comments: EDIS does not attempt to collect IIF from individuals outside of the user registration process, only allows the input of documents and does not control what information is contained in these documents.
35	**Does/Will the Web site *share* IIF with other agencies external to USITC, or other people or organizations outside USITC?** Note: If yes, specify with whom and for what purposes, and identify the data elements in the Comments column. If the category of personal information is not listed, please check "Other" and identify the category.	☐	☒	☐	**Comments:** Any agency may act as a user of EDIS, and access publicly available legal documentation. The system does not control what information is contained in EDIS public documents that are viewable by external users. For purposes of enforcement of certain legal orders issued by the agency, some confidential business information containing IIF is provided securely to DHS, Customs and Border Protection.
36	**Are rules of conduct in place (or will they be in place) for access to IIF on the Web site?** Note: If yes, identify in the Comments column all categories of users with access to IIF on the system, and for what purposes the IIF is used.	☒	☐	☐	☒ Users ☒ Administrators ☒ Developers ☒ Contractors For what purposes: **Comments:** User information is required during the registration process, whether users elect to electronically file legal documents through EDIS or want to read publicly available legal documents. IIF contained in scanned documents is not regulated. It is possible that IIF on an individual may be entered without the consent/knowledge of that individual, as part of the documentation compilation and filing processes.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
37	**Does (or will) the Web site contain links to non-federal or state websites external to USITC?** Note: If yes, note in the Comments column whether the system provides a disclaimer notice for users that follow external links to Websites not owned or operated by USITC.	☐	☒	☐	☐ Disclaimer notice for all external links
	Administrative Controls				
Note**: This PIA guide uses the terms "administrative," "technical," and "physical" to refer to security control questions—terms that are used in several federal privacy laws when referencing security requirements. USITC recognizes the slight difference in terminology used in this guide from those that are used in other documents such as those published by the National Institute of Standards and Technology (NIST).**					
38	**Has the system been authorized (or will it be authorized) to process information?** Note: If yes, please identify when the authorization was provided. If an interim authorization to operate has been given, please indicate this in the Comments column.	☒	☐	☐	
39	**Have there been significant changes to the system since it was last certified and accredited?** Note: If the system has not been certified and accredited at the time of this PIA, please describe in the Comments column the plan and timeline for conducting a certification and accreditation (C&A) for this system.	☐	☒	☐	
40	**Are security controls routinely reviewed (or will they be)?**	☒	☐	☐	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
41	**Is there a system security plan for this system (or will there be)?**	☒	☐	☐	
42	**Is there (or will there be) a contingency (or backup) plan for the system?**	☒	☐	☐	Although there is a backup process to support restoration activities, a contingency plan will be documented.
43	**Are files backed up regularly (or will they be)?**	☒	☐	☐	
44	**Are the backup files stored off-site (or will they be)?**	☒	☐	☐	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
45	**Are there user manuals for the system (or will there be)?**	☒	☐	☐	http://www.usitc.gov/docket_services/documents/EDIS3UserGuide-External.pdf
46	**Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the IIF being collected and maintained (or will they be)?**	☒	☐	☐	
47	**Who will have/has access to the IIF on the system?** Note: Check all that apply in the Comments column.				☒ Users- this includes USITC employees and the public ☒ Administrators ☒ Developers ☒ Contractors ☐ Other:
48	**If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?**	☒	☐	☐	

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
49	**Are methods in place to ensure least privilege (i.e., "need to know" and accountability) (or will there be)?** Note: If yes, please specify method(s) in the Comments column.	☒	☐	☐	USITC staff office directors and their designees authorize privileges to internal users based on least privilege principles.
50	**Are there policies or guidelines in place on the retention and destruction of IIF (or will there be)?** Note: If yes, please provide some detail about these policies/practices in the Comments column.	☒	☐	☐	The USITC Records Disposition Schedule governs the retention and disposition of documents on EDIS.
	Technical Controls				
51	**Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system (or will there be)?** Note: If yes, check all that apply in the Comments column.	☒	☐	☐	☒ User ID ☒ Passwords ☒ Firewall ☐ Virtual Private Network (VPN) ☐ Encryption ☒ Intrusion Detection System (IDS) ☐ Common Access Cards (CAC) ☐ Smart Cards ☐ Biometrics ☐ Public Key Infrastructure (PKI) ☐ Other E-Authentication ☒ Other: Two-factor authentication for USITC personnel accessing the application off-site.

No.	Privacy Question Sets	User Response			Comments
		Yes	No	N/A	
52	**Are any of the password controls listed in the Comments column in place (or will they be)?** Note: Check all that apply in the Comments column.	☒	☐	☐	☒ Accounts are locked after a set period of inactivity. ☒ Minimum length of passwords is configured. ☒ Passwords must be strong. ☒ Accounts are locked after a set number of incorrect attempts.
53	**Is a process in place to monitor and respond to privacy and/or security incidents (or will they be)?**	☒	☐	☐	
	Physical Controls				
54	**Are physical access controls in place (or will there be)?** Note: If yes, check all that apply in the Comments column.	☒	☐	☐	USITC employees and contractors are issued badges and are provided secure proximity access to workspace.
	- END -				

PIA Contact Information

Please address all comments to the Senior Agency Official for Privacy at:

U.S. International Trade Commission
500 E Street, SW, Suite 316
Washington, DC 20436
(202) 205-2000
Please direct e-mails to the EDIS Help Desk – edis3help@usitc.gov – with "Please direct to SAOP" in the Subject Line.

Appendix B: Glossary

Administrative Safeguards — Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.

Availability — Ensuring timely and reliable access to and use of information.

Certification and Accreditation (C&A) — A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Confidentiality — Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Cookie — A piece of information supplied by a web server to a browser, along with requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests.

General Support System (GSS) — An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Information in Identifiable Form (IIF) — Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means; information permitting the physical or online contacting of a specific individual

Integrity — Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Major Application (MA) — An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Persistent Cookie — A cookie that is stored on the user’s hard drive and remains there until the user deletes it or it expires.

Privacy Impact Assessment (PIA) — A process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

Record — Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. (See 5 U.S.C. §552a(a)(4))

Routine Use — With respect to the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected.

Session Cookie — Technology that is used to facilitate a visitor's activity within a single session and does not persist over time

Significant Change — Any change that is made to the system environment or operation of the system. Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to:

- installation of a new or upgraded operating system, middleware component, or application;
- modifications to system ports, protocols, or services;
- installation of a new or upgraded hardware platform or firmware component; or
- modifications to cryptographic modules or services.

Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

Stand-alone System — A system that is neither network-connected nor connected to any other system or group of systems.

System — A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information

System of Records — A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual

Technical Controls — The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Website — A collection of interlinked web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the website.