Federal Trade Commission
Privacy Impact Assessment

Registered Identification Number System (RINS)

January 2017

(Reviewed April 2019)

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

A. Overview

The Federal Trade Commission (FTC) is an independent federal agency with a mission to prevent business practices that are anticompetitive, deceptive, or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity.

In support of this mission, the FTC's Bureau of Consumer Protection (BCP) oversees and enforces rules issued pursuant to various federal product labeling laws, including the Textile Fiber Products Identification Act, the Wool Products Labeling Act, and the Fur Products Labeling Act. Under those Rules, the staff of BCP's Enforcement Division (ENF) administers the Registered Identification Numbers Program (RN Program), issuing Registered Numbers (RNs) to U.S.-based businesses that wish to use RNs to identify the company that manufactured, imported, distributed, or sold a covered textile, wool, or fur product.[1] Businesses residing in the United States use these RNs on product labels as a simple, shorthand method of identifying themselves in compliance with federal product labeling laws.

ENF staff utilize an electronic system of records, the Registered Identification Number Systems (RINS), to administer the RN Program. Specifically, ENF staff use RINS to record the RNs associated with businesses, facilitate public searches for RNs, provide the public with identifying information for each business that has obtained an RN, act on requests to obtain new RNs, update existing RN records, and cancel RNs. RINS contains data on tens of thousands of RN numbers. In recent years, the FTC has issued approximately 3,000 RNs per year. RINS contains largely non-sensitive, publicly-available business information sent to the FTC by submitters who have requested RNs.

RINS has been upgraded to a new web-based interface. RINS has two chief components, a public interface and an FTC staff interface. The following paragraphs describe these components in further detail.

B. Public Interface

The public website interface is used in two basic ways: (a) businesses can apply for, update, or cancel their RNs; and (b) businesses, consumers, staff, and law enforcement can search the online RN database to find the owners of RNs.

Businesses that apply for or update their RNs provide largely non-sensitive, publicly-available business information that is stored within RINS. There are less than two dozen data fields associated with each RN number application or record. The information collected and maintained in RINS consists of the legal name of the business that wishes to use an RN; the name(s) under which it does business; the legal form of the business (corporation, partnership, etc.); the business' physical address in the United States and its mailing address; the type of business it conducts (manufacturing, importing, etc.); its external contact information (telephone number,

[1] *See, e.g.*, 16 C.F.R. § 303.20 (describing RN Program).

email address, and in some cases, fax number and/or Internet URL address); the business' product lines that render it eligible for an RN (e.g., cloth, wool, or fur coats); and the name and title of the business officer who certifies the information submitted to the FTC for a RN.

The public interface supports a search function that allows the public to construct basic and Boolean searches and to review and print the results. Visitors to the website can use the public interface to search RINS data and locate the source or distributor of specific products. For example, a dry cleaner could use the website to identify who put care instructions on a particular garment. Or an interested consumer could type an RN number into a website to trace a certain dress to a particular bridal shop or whichever company supplied the bridal shop. Another example might be a police investigator using the website to help find background information on a garment worn by a crime victim. RN information also could be sought in disputes concerning garments' alleged safety hazards or flammability. Some data fields from the RN application form are not displayed in response to public website searches for privacy reasons: the name, phone number, fax number, and email address of the business officer who certified the information submitted to the FTC, and the physical address of sole proprietors who have also provided a mailing address to the FTC (the mailing address is displayed instead). However, the information not displayed in response to a search may be made available in response to a Freedom of Information Act (FOIA) request.

C. FTC Interface

After U.S.-based businesses apply to obtain, update, or cancel RNs using the public web interface, ENF staff use RINS to review those applications and to generate responses to such requests. RINS also supports reporting functions and facilitates FTC disclosures in response to FOIA requests and to other entities, as permitted by law. For example, using RINS' reporting function, ENF determined that in fiscal year 2014, the FTC issued nearly 3,000 RNs, updated over 400 numbers, and cancelled 17 numbers. Aside from administrative functions, the FTC interface offers the same types of tools available via the public interface. As with the public web interface, ENF can use RINS to determine if an applicant already has a RN, search RINS to identify the owner of a RN that appears on a garment label, and to print information.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The following legal authorities allow for the collection, maintenance, and dissemination of the information for the RN Program and RINS:

- The Federal Trade Commission Act, 15 U.S.C. §§ 41-58;
- The Fur Products Labeling Act, 15 U.S.C. §§ 69 - 69j;
- The Textile Fiber Products Identification Act, 15 U.S.C. §§ 70 - 70k;
- The Wool Products Labeling Act of 1939, 15 U.S.C. §§ 68 - 68j;
- Rules and Regulations Under Fur Products Labeling Act, 16 C.F.R. § 301.26;
- Rules and Regulations Under the Textile Fiber Products Identification Act, 16 C.F.R. § 303.20;
- Rules and Regulations Under the Wool Products Labeling Act of 1939, 16 C.F.R. §§ 300.4, 300.13.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address (Business)		☐ Other *(Please Specify)*:
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☒ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

RINS and the RN Program collect, use, and maintain the following publicly available data, consisting of business information: the legal name of the company that has requested or obtained an RN; the RN issued to the company, where applicable; the name under which the company does business; the legal form of the company, (i.e., corporation, limited liability company, etc.); the type of business conducted by the company, i.e., distributorship, importer, etc.; the product line for which the company has requested or obtained an RN, i.e., men's apparel or women's apparel, etc., and including whether the product line contains wool, fur, or textile; and the URL of the company's website. Businesses are already required to identify themselves on product labels in accordance with federal law, and voluntarily submit the above information if they wish to use an RN to comply with the identification requirements of relevant federal labeling laws.

RINS also records certain administrative information that is non-PII: the date and time of requests received from the public and the date of actions taken by FTC ENF staff in regard to

[2] Per OMB Circular A-130, 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.

such requests; and whether such requests have been referred from one ENF staff member to another for action (e.g., approval, rejection, or other response to an RN request).

2.3 What is the purpose for collection of the information listed above?

FTC collects the information listed above in furtherance of administrating the RN Program in compliance with federal laws and regulations relating to the public identification, on product labels, of U.S.-based businesses engaged in the manufacture, importing, distribution, or sale of textile, wool, or fur products. Federal regulations restrict issuance of RNs to qualified entities, residing in the United States, that submit the information collected to the FTC. *E.g.*, 16 C.F.R. § 303.20(a), 16 C.F.R. § 303.20(d) (RN application form listing information fields now collected in RINS). Accordingly, the information collected is limited to that relevant and necessary for the administration and oversight of the RN Program, and the issuance, updating, and cancellation of RNs through RINS.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
Commercial Entities	The FTC accepts requests for RNs, and requests to update RN information or cancel RNs, from commercial entities. These entities provide basic company information (e.g., physical address, mailing address, email address, URL) and a brief description of their product line that qualifies for issuance of an RN (e.g., a textile, wool, or fur coat). The information is submitted by a company officer, who provides their name and title, and certifies that the information is correct. The submission occurs electronically through RINS and data is encrypted; the RINS website includes SSL encryption, and the data is also encrypted in the SQL server database. Sometimes (though significantly less often) data may be submitted by mail or fax submission to ENF. Applying for an RN is completely voluntary. Submitted responses are maintained for response by ENF and thereafter for the recordkeeping and identification purposes of the RN Program, so that members of the public and others may search RINS to determine what commercial entity registered a particular RN.
FTC Staff	FTC staff authorized to access RINS can perform data entry, *e.g.,* inputting information that commercial entities mailed or faxed to the FTC. This information may consist of any of the data fields described in Section 2.1 and 2.2 above. Additionally, FTC staff act to approve, reject, and respond to requests for RNs, and requests to update RN information or cancel RNs, from commercial entities. RINS records these events when they occur.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC ENF Staff	FTC ENF staff have access to the data in RINS for the purpose of administering and overseeing RINS and the RN Program. FTC staff access the data via the FTC network. FTC users must have authorized accounts that require a valid username, password, and permissions granted to access RINS in order to view and perform actions in RINS. RINS access is limited to a small number of FTC ENF staff, typically between 5-10 persons, who are assigned to manage the RN Program and have a demonstrated business need to access the system or oversee its use. Access is terminated when an ENF staff member is no longer assigned to work or on oversee the RN Program.
FTC OCIO Staff	A limited number of FTC Office of the Chief Information Officer (OCIO) staff have access to the data in RINS for the purpose of overseeing technical aspects of RINS and maintaining its operative condition.
FTC Contractors	A limited number of FTC contractors have access to the data in RINS for the purpose of assisting FTC OCIO Staff and ENF Staff in maintaining RINS in operative condition and responding to requests to perform maintenance on the system. Access is terminated when the contractor is no longer responsible for performing such duties.
Businesses	Businesses access the system to apply for, update, and cancel their RNs.
Members of the Public (Consumers)	Visitors to the website can use the public interface to search RINS data and locate the source or distributor of specific products.
Law Enforcement Entities	Law enforcement entities can search the online RN database to find the owners of specific RNs or to gather background information on a labeled item. Law enforcement entities have access to the same information in RINS as general members of the public.

3.2 If contractors and/or third party service providers have access to data in the project/system, explain what, if any, privacy requirements are in place to ensure that data is properly protected.

☐ Not Applicable

OCIO contractors may be authorized to access data in RINS to perform technical support relating to the development and maintenance of the system. The contractors are bound by non-disclosure agreements prohibiting unauthorized disclosure of information collected by the FTC. The contractors also are required to take the FTC's Security Awareness and Privacy Training course before being granted access to the FTC network, and annually thereafter to maintain access privileges.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☐ Other (*explain*):

☐ Notice is not provided (explain): _____

The login banner on the website states the following:

"You are accessing a U.S. Government information system, which is provided for U.S. Government-authorized use only. By using this system, you understand and agree to the following: "(1) unauthorized or improper use of this system, may result in the revocation of access privileges, as well as possible civil and criminal penalties, (2) users have no reasonable expectation of privacy or other right of privacy in this system including in any communications or data stored on or transmitted through the system and, (3) use of this system whether authorized or unauthorized constitutes consent to the scanning, monitoring, interception, recording, reading, copying, capturing, disclosure or use of, communications or data stored on or transmitted through this system, at any time and for any lawful government purpose, including but not limited to, monitoring network operations, quality control, or employee misconduct, law enforcement, and counterintelligence investigations."

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Applying for an RN is strictly voluntary. If a company chooses to do so, some basic business information fields must be completed. If a company elects not to apply for an RN, the company may still comply with federal labeling laws that cover various textile, wool, or fur products by identifying themselves by name on their product labels in compliance with the specific requirements of the applicable statute(s). Companies that submit their information consent to all legal uses of that information, but have the opportunity to decline to provide any information.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Businesses and other entities have ready access to their information stored in RINS. The general purpose of the system is to make available to the public the identifying information for companies responsible for various textile, wool, and fur products bearing product labels. Businesses and

other entities may visit the FTC's website, obtain login credentials for RINS, and login to RINS to go beyond searching RINS data records and actually access, revise, and submit updates to their own information on file in RINS. RINS issues login credentials in response to public requests as follows: In obtaining login credentials, the person requesting such credentials must supply a valid email address and respond to an automated email to that email address, authenticating that they have access to that email account. RINS also requires users to specify a password for logging into RINS. After logging into the system, users may submit updates to their own information on file in RINS.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As explained in 4.3 above, businesses and other entities may visit the FTC's website, obtain login credentials for RINS, and login to RINS to access, revise, and submit updates to their own information on file in RINS. Additionally, they may submit complaints, concerns, or questions to the ENF staff responsible for the RN Program at RN_admin@ftc.gov. It is not necessary to have RINS login credentials in order to submit a complaint, concern, or question to this email account, which is regularly monitored on FTC business days.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

FTC ENF staff receive requests for new RNs as well as requests to update and cancel RNs. Using RINS, ENF staff verify that the information submitted meets the data requirements of the rules implementing the RN Program. E.g., 16 C.F.R. §§ 300.4, 300.13 (wool); 16 C.F.R. § 301.26 (fur); 16 C.F.R. § 303.20 (textile). For example, an applicant who fails to provide a valid U.S.-based street address may be rejected. RINS validates U.S.-based street addresses against those on file with the United States Postal Service (USPS), and ENF staff may ask submitters of non-conforming addresses to provide a valid physical address or explain the discrepancy, to confirm that the applicant resides in the United States and is thereby qualified to obtain an RN. Incomplete submissions, such as one not certified by a company officer, are returned or rejected – in some cases, automatically, as RINS identifies multiple fields as required fields and does not accept requests where required data (e.g., legal business name) are absent.

As a "directory" that helps businesses identify themselves in compliance with federal product labeling law, the responsibility for submitting maintaining accurate, reliable information in RINS rests with the businesses that requested and obtained RNs. It is the RN holder's responsibility to ensure their data remains current. RNs are subject to cancellation if the RN applicant or holder does not promptly notify the FTC of any changes in name, business address, or legal business status of the entity to whom an RN has been issued (e.g., 16 C.F.R. § 303.20(3)).

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

RINS exists to make business identifying information available to the public. Accordingly, all members of the public can search for information relating to RNs. However, there are safeguards in place to protect the information in RINS, and controls to ensure proper use of the data.

For the public interface, only authenticated RINS users with passwords can update and submit requests to change data on file. Passwords are required to be complex and hash encrypted with an additional random string added, so passwords cannot be guessed from encrypted text. Users may change their passwords as often as they wish, but are not required to change passwords at predetermined intervals.

The internal FTC RINS interface uses forms authentication and restricts access to only those authorized users with a demonstrated business need to utilize the system. Access requests must be approved by FTC management. Events are stored in the database for any action taken in the system by any user, including the modification of data, and the identity of the user who modified data is stored in RINS' events history table. This mechanism can be used as an auditing tool within the system. Any changes executed by internal users are logged within the system and maintained indefinitely to provide an accurate historical record of events.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

No live PII data is used in the course of testing, training or research. Fictionalized, dummy data is used, if and when necessary.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

RINS is intended to be a permanent directory and record of RNs issued by the agency, some of which date back decades and are still in use. To identify the businesses responsible for older articles put into commerce, RINS contains historical data. Accordingly, these records are not routinely destroyed according to a retention schedule.

RN databases will also have historical data of all the RNs; there is currently no mechanism to delete the RN history data. RN data is not purged from the system as RNs are intended to provide a permanent record. However, users may cancel their registrations at any time; if a registrant deletes their login account, their user ID and password is no longer needed and is therefore deleted from the system. The textile information, however, continues to be maintained in the system to account for garments that have been manufactured and sold with that registration number.

The archiving of information within the system occurs with a transfer of the system data and appropriate documentation to the National Archives and Records Administration (NARA) every five years, and within one year after the system has been decommissioned. This does not include system user metadata (i.e., user ID, passwords), which is deleted if and when users delete their accounts.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

RINS uses both an external and an internal website. It uses ASP.net session in the external and internal interfaces to store and retrieve values for a user as the user navigates through ASP.NET pages in a web application. The information is stored in the web server's memory, and the information is passed between the server and users using a unique encrypted session ID. This method saves user information in server memory while an internally secured and encrypted, randomly-generated session ID number is stored on the user's machine in Random Access Memory (RAM). The client retrieves the user information from the server using the session ID number as the user navigates through the site.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Information contained in RINS may be inaccurate.	With the most recent RINS upgrade, all RN holders with an email address on file receive an email inviting them to log into the system and review and correct their information if needed. All future RINS users will be required to create new login accounts as the previous legacy system did not have a login functionality. RINS also permits users to update their information as needed in the future; failure to maintain accurate information subjects the holder to possible cancellation of their RN. ENF system administrators can manually correct errors in the system. Additionally, system administrators use and monitor the system regularly and can report and obtain repairs for system issues that may affect data integrity.
Users or members of the public may access PII contained in RINS.	Certain data fields containing PII are not displayed when a consumer searches the public website. For example, the name, phone number, fax number, and email address of the business officer who certified the information submitted to the FTC, and the physical address of sole proprietors who have also provided a mailing address to the FTC (the mailing address is displayed instead). Likewise, users must create a RINS account before they can enter or alter data in the system. RINS requires email address and password validation for all

Risk	*Mitigation Strategy*
	users. Users may only enter or alter data for RNs associated with their own account.
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	ENF system administrators strictly manage access control and limit the use and access of all data to purposes for which it was collected. A system log is maintained that reflects who accessed the data at any given time, and whether the data was tampered with or edited. Changes to data are logged to identify the user responsible for the changes.
An individual may enter sensitive information in the free text field.	System administrators have the ability to access individual records and delete information as necessary, including sensitive information that may be inadvertently submitted, such as SSNs, for example. If users provide sensitive information – which is not required to use RINS – the system administrator ensures the information is deleted as it is not necessary for the purposes of this system. System administrators check for sensitive data while processing requests and reviewing approved requests and remove the data as necessary.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

RINS is designed with built-in privacy controls, including email address and password verification for all users. Users attempting to log into the public interface are locked out after five unsuccessful attempts to login. Users cannot obtain login credentials in the first place without authenticating that they have access to a valid email address. Additionally, the system supports having one user associated with an RN, and if the email address of the user associated with an RN changes, a notification is sent to the email addresses previously associated with that RN to notify that email address that a new email address has been associated with the number. The RINS events table logs changes to data in the system by user and date/time.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Not applicable. Records are searched and retrieved from the RINS database using the publicly available search engine posted at www.ftc.gov, which permits queries by RN Type, RN Number, Company Name, Business Type, City, State Code, ZIP, and/or Product Line. Because these records are not retrieved by individual name or any other identified personally assigned to an individual, the records do not constitute a system of records within the meaning of the Privacy Act of 1974, and there is no applicable FTC SORN for this system.

To the extent the system collects, maintains, and retrieves PII in the form of user ID and other login credentials assigned to individual users in order to verify, control, and log their access to the system, FTC SORN VII-3 (Computer Systems User Identification and Access Records – FTC) applies to that data. The FTC's SORNs are made available to the public via the FTC's SORN page.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

By design, RINS contains restrictions on the collection, use, and maintenance of information, such as the aforementioned password controls and collecting only that information needed to process RN-related requests. External checks are in place as well, as access to the FTC interface is restricted by agency management to agency personnel with a demonstrated business need to use the system. RINS supports auditing; its events table logs the event type, the modified data, and the user responsible for modifying data when a change occurs. While RINS is designed to make basic identifying information for businesses available to the public, the system's design and use mitigates against the relatively modest privacy risks associated with its operation.