

iTRS URD for VRS System - Privacy Impact Assessment

Application Name:	iTRS URD System
Date:	September 1, 2020

Record of Approval

Document Approval		
Document POC		
Printed Name: Allan Jacks	Title/Role: CISO/Privacy Officer	
Signature: /s/	Date: 6/21/2021	
Approval Structure		
Printed Name: Sean Bull	Title/Role: COO/Authorizing Official	
Signature: /s/	Date: 6/9/21	

Record of Approval

Date	Description	Author
August 10, 2020	Initial assessment drafted	Samuel BowerCraft
June 8, 2021	Business owner signoff	Amanda Coby

*Document created based on template from Federal Communications Commission (FCC) Information Technology (IT) department.

Introduction

Section 208 of the E-Government Act of 2002^[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and will not be made available to the public. The PIA was intended to be a tool to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"^[2]

Under the FCC contract Rolka Loube is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

In accordance with FCC policy, system owners should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The IPA helps system owners determine whether their systems will collect the kind of information that would make them subject to the requirements of Section 208. The PIA should not be completed if the IPA has not yet been completed first since it determines if your system requires a PIA.

If you have any questions, please contact ITSecurity@rolkaloube.com

[1] 44 U.S.C. § 3501 note.

System Overview

1	Avoiding technical terms and unexplained abbreviations, please provide a general description of this information system.	The VRS User Registration Database is a system that houses known registered users who have been confirmed to use the VRS system. Providers submit supporting details for each registered user to populate the database; this information is subsequently reviewed and vetted by the company to confirm accuracy and completeness. The system provides identity validation for evaluation of compensation for calls made by the VRS system.
2	Is this a new information system or a significant revision of an existing system?	<input checked="" type="checkbox"/> New System <input type="checkbox"/> Revision of Existing System:
3	What is the purpose of this system?	The URD system is used to register eligible VRS users and to complete the identity validation process for each registration to subsequently use the VRS service. Providers perform an initial evaluation of eligibility and upload the data to the URD system. Rolka Loubé then evaluates the data against a third party system (Lexus Nexus) and makes an independent conclusion regarding the user's eligibility. Providers use the URD system to check and confirm ten digit telephone numbers for status and may review and update their own users' data on the URD.
4	If this system is going to be provided through a cloud-based computing system, ^[1] please check the box that best describes the service the FCC receives from the cloud computing provider: <hr/> ^[1] See NIST, <i>The NIST Definition of Cloud Computing</i> , Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final .	<input type="checkbox"/> The system is not cloud based. <input type="checkbox"/> The system uses provider-supported application(s) on the provider's cloud network (Software as a Service [SaaS]). <input type="checkbox"/> Rolka Loubé has deployed application(s) on the provider's cloud network and the provider supports the applications (Platform as a Service [PaaS]). <input checked="" type="checkbox"/> Rolka Loubé has deployed its own application(s) on the cloud network and controls how these application(s) are configured and operate (Infrastructure as a Service [IaaS]).
5	Under what legal authority is Rolka Loubé developing, procuring, or revising this information system?	Rolka Loubé has been awarded the contract to manage the TRS fund by the Federal Communications Commission (FCC); this system supports the confirmation of eligibility of users of the TRS system for their phone calls and subsequent disbursements to providers for eligible phone calls.

Nature and Use of the Information that will be Collected

1	Specify what types of personally identifiable information (PII) may be collected, maintained, or processed in this information system. Check all that apply and add any types that are not listed below.
<p>PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII, as needed.</p>	

<input checked="" type="checkbox"/> Full Name <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Home Address <input checked="" type="checkbox"/> Phone Number(s) <input checked="" type="checkbox"/> Place of Birth <input checked="" type="checkbox"/> Age <input checked="" type="checkbox"/> Race/Ethnicity <input checked="" type="checkbox"/> Alias <input checked="" type="checkbox"/> Sex <input checked="" type="checkbox"/> Email Address <input checked="" type="checkbox"/> Work Address <input checked="" type="checkbox"/> Taxpayer ID <input type="checkbox"/> Credit Card Number <input type="checkbox"/> Facsimile Number <input checked="" type="checkbox"/> Medical Information <input checked="" type="checkbox"/> Education Records <input checked="" type="checkbox"/> Social Security Number <input checked="" type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> Biometric identifiers (e.g., fingerprint, voiceprint) <input type="checkbox"/> Audio Recordings	<input type="checkbox"/> Photographic Identifiers (e.g., image, xray, video) <input checked="" type="checkbox"/> Certificates (e.g., birth, death, marriage, etc.) <input checked="" type="checkbox"/> Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.) <input checked="" type="checkbox"/> Vehicle Identifiers (e.g., license plates) <input type="checkbox"/> Financial Information (e.g., account number, PINs, passwords, credit report, etc.) <input type="checkbox"/> Geolocation Information <input checked="" type="checkbox"/> Passport Number <input type="checkbox"/> User ID <input type="checkbox"/> Internet Cookie Containing PII <input type="checkbox"/> Employment Status, History or Information <input checked="" type="checkbox"/> Employee Identification Number (EIN) <input checked="" type="checkbox"/> Salary <input checked="" type="checkbox"/> Military Status/Records/ID Number <input checked="" type="checkbox"/> IP/MAC Address <input checked="" type="checkbox"/> Driver's License/State ID Number (or foreign country equivalent) <input checked="" type="checkbox"/> Other (Please Specify): <ul style="list-style-type: none"> • Proof of residency • Tribal ID Number (TIN) 	
2	Please explain why it is necessary to collect these PII data elements to carry out the purpose of this system.	The information gathered is used to track and confirm the identity of users for the TRS program for the VRS service; the validation supports the evaluation of compensable services by providers who receive payment from the TRS fund based on eligible calls.
3	Will this PII be collected from individuals themselves, or from third parties?	Service providers collect the PII and submit the information and eligibility support to the system.
4	Will individuals be able to consent to the collection or particular uses of the information? What will the form of the consent be? What happens if individuals do not consent to the collection or particular uses?	Individuals may consent to not provide the information; in these cases the individual will not be entered into the system at the provider level and will not be provided access to services.
5	Please explain how these PII data elements will be processed or used in the course of operating this information system.	The information is used to identify individual users of the service, to confirm the evidence that validates their identity as required to use the service, and this information is used to evaluate compensability of phone calls by users of the service.
6	What steps will Rolka Loube take to make sure this PII is accurate, complete, and up-to-date?	Ongoing evaluation and vetting of the data in the system is the responsibility of service providers. Users may engage with service providers to confirm the accuracy of their information; service providers are responsible for updating the information in the application and have access to the data via a web application.
7	Are there procedures in place to allow individuals access to their PII or to correct inaccurate information?	No; individuals do not have access to this data set. Review by Rolka Loube and requests for updated information is sent to the providers. Providers may access the data they have provided to review its accuracy and request updates as needed.
8	How long will the PII be retained and how will it be disposed of?	The data in the application is maintained indefinitely based on direction from the agency.

Data Security

1	Are there administrative procedures and technical safeguards in place to protect the data in the system? What controls are in place to ensure proper use of the data?	Yes; access controls are in place that limit user access to the system and the user's rights within the system. Least privilege is applied to limit access on the system for both company users and provider access. Column level encryption has also been put in place to ensure the security of the PII stored within the database.
---	---	---

2	Has the system undergone the appropriate security risk assessment and received authority to operate?	An ATO for this system is anticipated to be issued as of September 30, 2021. The ATO project is currently underway in collaboration with the FCC.
---	--	---

Access and Sharing of the Information

1	Which Rolka Loube employees and contractors will have access to the PII in this information system?	Amanda Coby, Garrett McGrath, Brian Robinson, Dan Stolnik, Derek Coates
2	Will the information be shared with third parties as part of the operations of the information system (e.g., through an application programming interface or "API")?	The information is available for review by service providers; service providers have access to their own data through a web application.

Privacy Act System of Records Notice

1	Is the FCC planning to publish or has it already published a Privacy Act System of Records Notice (SORN) for this information system? If the FCC has already published a SORN, please provide a citation to the Federal Register.	<p>Yes</p> <p>System of Records:</p> <ul style="list-style-type: none"> o FCC/CGB-4, "Internet-based Telecommunications RelayService-User Registration Database (ITRS-URD) Program" o FR Doc. 2015-02530 Filed 2-6-15; 8:45 am
---	---	--