**RFP 21-2721 Identity Fraud Detection Services**

**INSTRUCTIONS**

***Instructions:*** *Please provide responses to the clarification question(s)/prompt(s) below. Information provided in the clarification responses will be considered as part of the respondent’s proposal. Where appropriate, supporting documentation may be referenced by specific page and/or paragraph number(s). If any of the responses contain confidential information, as defined by IC 5-14-3, please reference the attached confidential material and separate from the rest of this response document. Otherwise, a redacted version of this clarification document will need to be submitted.*

**DUE DATE: December 2, 2020 BY 3:00 PM EDT**

**RESPONDENT: Lexis Nexis Risk Solutions**

| **Clarification Question** | **Respondent Response** |
| --- | --- |
| What kind of information is needed from DOR to do your analytics on identities and/or to score them? | No additional information is required from DOR for LN to provide analytics on identities and/or score them. The current, automated batch process in place today gives us all the information from DOR that is needed to execute our analytics on identities (including individuals assigned an ITIN), as well as on the bank and IP metadata, email addresses and paid preparers when present. Nothing in our proposed solution changes that existing process in production today. The only thing that may be added, but is ***not*** required/needed, would be an input Driver’s License # if DOR has it for the taxpayer(s) on the return. |
| How often do you find data on taxpayers who were assigned an ITIN? | We find taxpayers assigned an ITIN on a daily basis. We currently have over 9.3 million Individual Taxpayer Identification Numbers (ITINs) identified within our database. We receive data on ITIN’s from multiple data suppliers and update that population daily, weekly, monthly depending on the source. The number of ITINs is constantly growing and being refined as we gain more data over time to continue to link disparate data to individuals, including ITINs, through our patented LexID process. |
| Please describe each of your implementations with GenTax. Specifically.   * What version of GenTax are they running? * What GenTax user functions are they able to utilize? * What LN User functions do they utilize? * Does the GenTax architecture inhibit implementation of any functions you have described in your proposal? | * Currently Alabama DOR is running version 10 of GenTax. The LNRS solution has been seamlessly integrated into AL’s income tax fraud enterprise program, in conjunction with GenTax, since 2015. LN has effortlessly been a part of AL/GenTax system upgrades throughout the years.      * AL DOR has always been able to utilize the full scope of GenTax functions, in addition to fully using the LN analytical and batch functions without interruption. If any GenTax functions were/are not utilized, it was/is due to resources, budget or other AL DOR constraints, not due to a lack of LN compatibility. * AL DOR regularly uses LN Accurint for Government and analytical platforms to augment the identity fraud detection automated batch process. Additionally AL DOR uses our identity authentication solution on a subset of tax returns. This RFP proposal follows the same successful pathway. * No, the GenTax architecture does not inhibit implementation of any functions described in our proposal. In fact, as noted on another question, LNRS has seamlessly improved our batch processes while harmoniously integrating multiple GenTax upgrades. No user interruptions have been noted over the years/upgrades. |
| You stated that the Accurint for Government product was available from any network/any device. Can we limit access by our users to state devices attached to state networks (SOI IPAs)? | Yes, you can absolutely limit access to your users on their state devices attached to state networks (SOI IPS’s). LNRS takes security of our solutions, and customers’ use thereof, very seriously. We have the proper security protocols in place to enable our customers to limit access by individual user to certain devices and/or networks (SOI IPAs). This is actually the norm to limit access by SOI IPAs. |