Respondent:	LexisNexis Risk Solutions

Instructions: Respondent(s) shall provide a written response to each of the questions listed below in the yellow text box. When stated, responses shall include all minimum response requirements and clearly indicate the applicable sub-bullet (e.g., a., b., c.) for all provided descriptions. Respondent(s) may find additional details surrounding referenced requirements within Attachment J – Scope of Work.

1	**Proposal Overview** Provide an executive overview of your proposal and describe your organization's ability to meet or exceed the requirements of this solicitation. Provide a high-level description of your organization's mission, vision and goals. Describe your organization's experiences and qualifications that demonstrate your unique capabilities to execute DOR's required services.

As a global company with a global reach, LexisNexis Risk Solutions (LNRS) is part of the larger RELX Group. With approximately 30,000 employees, RELX Group is a global provider of information and analytics professional and business customers across industries. The group serves customers in more than 180 countries and holds offices in 40 countries. LNRS connects the dots between billions of public records in transactions, resulting in actionable information our customers use to advance their goal. Our vast data resources include over six terabytes of content comprising 87+ billion public and proprietary records. Our big data technology includes a proprietary supercomputing platform that enables processing at very high speeds. To create an accurate view of an individual or business, we leverage a unique identifier with our patented linking technology known as LexID. The technology uses scalable automated linking technology, a proprietary and patented method of linking and clustering data. This persistent link illuminates false positives and builds an extremely comprehensive and accurate representation of identities that matter.

LNRS believes in the power of data and advance analytics for better risk management. We are the industry leader in data analytics and a top provider for organizations to get actionable insights to manage risks and improve results. As DOR's existing provider of Identity Fraud Detection Services, we are a leader in data analytics and technology. We leverage our industry leading big data computing platform with vast data assets and a proprietary technology to enable agencies to better analyze and understand data at scale. We reduce the time it takes you to reach results and decisions. LNRS enables customers to transform risk decision making and helps them fight fraud, facilitate compliance, streamline workflows and increase efficiencies . We proudly provide solutions for many markets on all levels for local, state and federal governments and their agencies. These markets include tax and revenue, communications, media services, financial services, insurance, collections and recovery, retail, and health care.

Our solutions help customers solve challenges such as identity authentication, detecting and preventing fraud, maintaining compliance, streamlining due diligence, and increasing productivity and revenue. LNRS services customers across all industries in government. We work with Fortune 1000 and midmarket clients globally. Customers are in more than 100 countries and include the world's top banks, 100% of the top 50 U.S. banks, 78% of the fortune 500 companies, and 95 out of the top 100 personal lines insurance companies.

In a world of growing data, the protection of privacy and responsible use of data are paramount. Our products and services are designed to: reduce fraud, mitigate risk, make society safer, and most importantly safeguard your private data.

LNRS pioneered the identity-based tax refund investigative solution, formerly known as TRIS. It was the first off-the-shelf solution designed specifically to stop tax refund identity fraud and the only identity-based refund

fraud detection solution to receive a patent. LNRS introduced the solution to the government sector in January 2012 and has stopped hundreds of millions of dollars in identity-based tax refund fraud in a multitude of states. We have prevented fraud that was missed by every tax data warehouse vendor and system integrator, in every jurisdiction LNRS has served – regardless of the fraud detection techniques employed. This year, our solution has upgraded and has a new name – **the Risk Intelligence Network (RIN).**

LNRS Advantages

Through our unmatched, patented LexID linking and 45 years of deep identity data, we can literally see identity fraud happen, grow and evolve. This could be from stolen identities, manipulated personally identifiable information (PII), or even from the epidemic emergence of synthetic IDs. We merge this unique capability into our income tax refund analysis solution, RIN, , so the DOR can seamlessly find identity fraud based, in near real time, before sending out a tax refund.

A key differentiator is that RIN accesses the "identity network" of every individual to stop identity fraud. LNRS researches an identity far beyond input data an individual reveals on a tax form. To LNRS, an identity consists of a comprehensive network of information going back throughout the history of that identity's rightful owner. To effectively build a network around identities, you must have visibility into individuals in the United States legally and illegally. You must also have the linking, fusing, and analytic technology to perform identity resolution on terabytes of data. RIN for income tax refund analysis has it all.

LNRS has unmatched experience to understand that stopping identity-based tax refund fraud requires the ability to assess quickly and accurately the identity network of every State tax filer, as well as other components to the tax return. This can only be achieved by:

1. Combining patented identity analytics (LexID)
2. A vast repository of public records that sits outside of State data warehouses
3. World class scoring models

It takes all three to objectively and fully analyze the entire identity network of each individual refund filer allowed into systems. LNRS combines these three elements and thus discovers and stops identity-based tax refund fraud others have "passed through."

RIN scores records for direct risk attributes such as imaginary addresses, deceased, or incarcerated. However, RIN goes beyond these basic identity checks and assesses the whole tax filer's identity network and incorporates **high value data elements such as IP address metadata, bank institution data, and bank account ownership information** to determine identity authenticity and categorical fraud risk.

RIN uses the same patented high-performance supercomputing technology (HPCC) and patented identity analytics (LexID) employed by classified defense and intelligence agencies. We incorporate advanced statistical analytics and world class scoring to suppress or increase the number of flagged records that the DOR would act upon, based on its evolving risk threshold, which can change anytime. RIN uses LexID to look not just at the filer's PII, but the filer's entire identity network and all identity networks using that PII. For example, if a filer's PII is stolen and LNRS sees it used by multiple people, then that return will be flagged, even if the PII on the return matches perfectly. The identity is severely compromised, and the probability of someone using it to file a false refund is extremely high.

No competitive offering matches the expansive LNRS collection of identity data. While they may claim to incorporate public records data, they typically use a limited number of sources, such as utility and telecommunications data or they draw upon only one bureau's credit data. By contrast, LNRS provides more data (87+ billion records) across more types of information (IP address, bank account, SSN, relatives, utility, telecommunications, resident services files, consumer records, phone data, death records, and much more) that is aggregated from more individual sources (10,000+) than any other vendor in the world. We take this approach to provide more in-depth insight into individual identities as well as broader insight across the population as a whole, because our customers demand it. In fact, the company that developed the FICO credit score formula augments its data with LNRS public records.[1]

The company that developed the FICO credit-score formula augments its data with LNRS public records.[1]

LNRS understands that detecting and preventing identity-based fraud requires an industry-leading, aggressive, multi-layered approach based on identity resolution, identity analytics and scoring, taxpayer authentication, and ongoing analytics. This understanding and our experience will assist the DOR in making mission-critical decisions to detect, prevent, and deter fraud effectively. That same industry-leading, aggressive, multi-layered approach is applied as the "Trusted Taxpayer" is identified. The Trusted Taxpayer concept not only identifies the stolen and fabricated identities to eliminate them from this Trusted Taxpayer group, but also identifies the citizen whose identity should be trusted. LNRS shares the DOR's goal in processing the honest taxpayers refund/tax filing as timely as possible, with minimal impact to the citizen.

To meet the DOR's mission, the solution must go far beyond simple credit bureau data. In fact, any solution that relies primarily on credit data should be put into question. Recent studies show 70 million people are credit invisible, unbanked or under-banked. Every year consumers are encouraged to obtain their credit reports and check for inaccuracies because millions of people have identities stolen. The only way to achieve the best solution is via a model that includes the most data sources with the largest number of identities. LNRS provides coverage that is more robust for the credit invisible, unbanked and under-banked populations who would not appear in or would be missed by credit bureau data alone. This combination of credit and non-credit data provides timely, authoritative, and reliable insight into the widest range of people, allowing the DOR to consider all identities – not just those who have bank accounts or credit cards. The end result is DOR's having the most extensive view of identities available.

Advantage #1: Extensive, continually updated referential data – the basis for reliable linking

LNRS compiles the largest collection of U.S. consumer identity information available today. We leverage public and proprietary records, which are updated regularly from sources including credit headers, utilities, phone directories, college directories, law-enforcement and more. This rich data set allows LNRS to understand the identity information for almost the entire U.S. adult consumer population (not just a subset of the credit active population) and provides the foundation of our ability to link consumers more accurately. The broad referential data coverage enables us to assess the uniqueness of different combinations of identity information and evaluate with confidence whether a record belongs to an individual.

This breadth of data enables LNRS to provide extensive coverage of the U.S. population, including people with thin (or absent) credit files and hard-to-reach population segments like the disadvantaged, unbanked and under-banked. It allows us to deliver actionable insight into:

[1] See http://www.washingtonpost.com/news/get-there/wp/2015/04/02/a-new-kind-of-credit-score-for-those-with-no-credit/.

- The wealthy, because they do not need to use credit to purchase goods and services.
- The poor, because they cannot obtain credit.
- 18- to 29-year-olds, who prefer to use debit or pre-paid cards rather than credit.[2]
- People recovering from financial setbacks who are working to rebuild their credit.
- Widows/widowers or divorced individuals whose credit histories link to their spouses' names only.
- Retirees without a mortgage.
- Individuals who prefer paying cash for everything and/or do not want to use credit.
- People using false identities to defraud the government – particularly those using deceased, foreign, and synthetic identities.

With LNRS, the DOR can be confident it is gaining insight into the widest range of demographics and geographic areas. The data coverage provided by LNRS allows DOR to automate the validation of more tax returns, prevent more fraud attempts, reduce false positives and process the honest taxpayers refund/tax filing confidently and efficiently.

Advantage #2: Superior Linking Technology

LNRS utilizes LexID, a proprietary, multi-patented data linking approach that draws upon our extensive referential data, links this information to the correct individual, and assigns a unique, reliable, secure identifier. The process involves running billions of complex statistical analysis and data comparisons to make more accurate matches. Core to the linking algorithms is "specificity" – the measure of uniqueness assigned to each value of data (e.g., name, DOB, etc.), to each field of the database, and to each combination of those values (e.g., name + DOB). This allows LNRS to identify when records have sufficient evidence to match confidentially. This sophisticated matching capability also accounts for variations in the way that data is represented (e.g., mis-keyed information, nicknames, etc.). This linking approach allows our LexID technology to resolve identities with up to 99.9% precision.

Above: LNRS data and linking LexID technology empowers you to quickly pinpoint synthetic and deceased identities.

LexID allows LNRS to recognize synthetic identities – allowing agencies to properly determine whether or not that person exists – before paying a refund.

Link Charts: RIN takes it another step further with Link charts. They allow for evaluating the information used by the identity. For example, RIN evaluates the information used by John Doe to see if people besides John are using the same information. This helps you uncover information such as: whether someone else is using the same bank account number used by John; whether someone else is using the same email address used by John; and have they used the same tax preparer. Information like this, when visually represented, makes it easy for investigators to identify if a bigger fraud ring and collusion exists.

Advantage #3: Holistic Evaluation

RIN goes beyond evaluating an independent tax return. It evaluates risk at another level up, at an identity level. RIN helps review all the tax returns tied to an Identity. Evaluating a tax return independently – such as "did the information on the tax return change from the last filing – is valuable but doesn't provide the

[2] Charisse Jones, "A Third of Millennials Have Never Had a Credit Card," *USA Today*, April 15, 2015. http://www.usatoday.com/story/money/2015/04/15/a-third-of-millennials-have-never-had-a-credit-card/25777653/

complete picture. RIN tracks the identity and links the tax filings to the identity through time. This maintaining of tax return history will help uncover any suspicious activity that occurred with that subject and saves investigators time going spent going through all tax returns that haven't been linked to an identity. Additionally, RIN takes it another step further with Link charts, allowing for evaluating the information used by the identity. For example, RIN evaluates the information used by John Doe to see if people besides John are using the same information. This helps you uncover information such as: whether someone else is using the same bank account number used by John; whether someone else is using the same email address used by John; and have they used the same tax preparer. Information like this, when visually represented, makes it easy for investigators to identify if a bigger fraud ring and collusion exists.

Advantage #4: Known Risk
Tax agencies typically conduct investigations and identify fraudulent tax returns and subjects as confirmed fraud. RIN takes this information and flags any new tax returns or identities that are re-filed later with the agency. This saves you a lot of research needed to identify manually any matches with known fraudsters. There is also a provision where known fraudsters' information can be shared across agencies. Other agencies can see tax returns submitted by fraudsters in a neighboring state.

Advantage #5: Experience
We proudly provide solutions for many markets on all levels for local, state and federal government agencies. These markets include communications, media services, financial services, insurance, collections and recovery, retail, and health care. This private and public experience allows LNRS to have unmatched depth and breadth of experience. Only LNRS is uniquely positioned to offer a combination of experience, patented technology, advanced data driven identity analytics, risk scoring, security and privacy compliance, and information on more individual identities than any other vendor does.

Key Benefits to DOR

The following table highlights features of the proposed LNRS solution and a few of the many benefits to DOR:

LNRS Solution Feature	Benefit to DOR
More than 87 billion public and proprietary records on more than 285 million identities	A comprehensive, 360-degree view into individuals
Information drawn from more than 10,000 data sources, including all three credit bureaus, utilities, registrations, consumer files, and more	Results for the widest range of the population, including demographics for which there may be little to no traditional credit or public records data
Proprietary linking technology (LexID) that resolves identities with up to 99.9% precision	Authoritative results despite aliases, misspellings, nicknames, multiple SSNs, and other variations
Over 270 million transactions processed per hour, with over 100 million identity-proofing transactions daily.	A highly efficient and widely entrusted solution with proven technology and capacity to support consistently large volumes of usage
Highly customizable configurations that provide a range of risk tolerances and index scoring models	Results that directly mirror DOR's unique requirements for a custom Risk Score
Exclusive bank institution data and bank account ownership information	Verifying bank account ownership reveals whether the taxpayer owns the account to which the funds are being directed
Includes internet address metadata as just one form of Digital Assessment	IP address reveals location and is the taxpayer trying to remain anonymous by using a proxy server or the TOR network

Exclusive Geo-Triangulation technology to reveal mismatched geography among tax return data elements	Proprietary logic to instantly assess the risk among taxpayer address, IP address and bank location that more often accompanies fraud returns
An expansive library of nearly 70 dynamic "out-of-wallet" quiz questions and the ability for DOR to create custom questions from DOR's internal proprietary data repository	Secure identity authentication using questions uniquely tailored to people's backgrounds
Off-the-shelf support for identity authenticating in English and Spanish, plus the ability to support additional languages upon request	Effective engagement of diverse linguistic groups among the more than 20% of the U.S. population that speaks English as a second language or speaks no English at all
Select to send a One Time Passcode (OTP) as a safe and efficient alternative citizen authentication option	After validating that the phone number belongs to the citizen, send an OTP via SMS, email or voice options, to give Treasury excellent control of the citizen experience.

2	**Mandatory Requirements** Provide acknowledgement that you meet or exceed the mandatory requirements referenced in Section III of the SOW and outline how you meet these requirements. At minimum, responses shall: 1. Describe your experience in serving federal or state identity tax fraud services over at least the last four years. Provide specific examples indicating how you meet this mandatory requirement. 2. Provide an example of how you have served and provided identity tax fraud services to another state or federal taxing authority within the last three years who requires the need to process up to 150,000 records daily.

LexisNexis Risk Solutions (LNRS) exceeds all mandatory requirements.

LNRS has provided investigative research services for 45 years and identity verification, fraud analytics and risk scoring and authentication solutions for 18 years. Customers across government, financial services, banking, retail, insurance, health care, telecommunications, and utilities industries use LNRS identity management solutions. These solutions are managed on a highly available and scalable platform that supports more than **270 million transactions processed per hour** for thousands of customers and processes more than **100 million identity-proofing transactions per day**.

LNRS is an identity company whose industry leading and patented identity solutions are leveraged by all 50 states, 70% of local governments and nearly 80% of federal agencies. Every day, federal government agencies responsible for securing our nation along with thousands of state and local law enforcement agencies trust LNRS to take their data and our data and perform advance analytics when lives matter. Examples include helping identify the 9/11 hijackers and their associates, the D.C. sniper, the Times Square bomber, and the Boston bomber. **We are also very proud our world-class identity analytics have helps rescue hundreds of children per year in partnership with the National Center for Missing and Exploited Children.**

This same technology powers our RIN solution. Through RIN's predecessor, introduced to the market in 2012, LNRS offered off-the-shelf solution designed specifically to stop tax refund identity fraud and the only identity-based refund fraud detection solution to receive a patent. LNRS has stopped hundreds of millions of dollars in identity-based tax refund fraud in multiple states. **The DOR has been one of our important, valued customers for over seven years.**

Examples of Relevant Experience

Indiana Department of Revenue (DOR)

In 2012, the DOR was searching for a vendor to satisfy the state's need for identity confirmation services. Included in the request were the following objectives:

- The ability to identify potential false or misused identities in tax returns.
- A confirmation process for a taxpayer to confirm that taxpayer's identity.
- An investigative tool to provide a select group of DOR employees access to a large set of data about an individual for investigative purposes.

The DOR selected LNRS to provide a modernized identity verification and fraud prevention solution. LNRS confidently fulfilled the request for the solution. In early January 2013, LNRS provided an end-to-end solution to accomplish the optimal results in identity confirmation. By utilizing the front end, filtered solution of resolving identities against the vast collection of public record data, to administering a personalized verification/authentication quiz, LNRS has assisted IDOR in, "catching $88 million in bogus refunds" from 2013 to present. https://statescoop.com/four-years-of-monitoring-has-decimated-tax-fraud-in-indiana
The DOR desired a solution that would offer identity verification services, but with optional supplementary elements such as a pre-filter system based on established fraud criteria coupled with a fraud data and trend analytics component. **Utilizing LNRS, the DOR has been effective stewards of taxpayer money and provides state investigative staff access to critical information to allow Indiana to target potentially fraudulent claims, enabling them to focus their investigations on cases that will make the most efficient use of their limited resources.**

For an additional account on success with LNRS, we offer the following testimony of former Indiana Revenue Commissioner Mike Alley before the U.S. Senate Finance Committee detailed their success.

> The program used LexisNexis, a third-party commercial vendor, to screen the returns and note identity information such as name, address, social security number, or other identifier information that appeared suspicious. Processing of those returns screened as suspicious was suspended and an identity confirmation quiz request was sent to the taxpayer at their filing address. Taxpayers were asked to confirm their identities by completing a short quiz. They can log into a secure web site or could call our call center where we had dedicated analysts to handle their quiz. As a result of implementing this pilot effort the department expected to directly reduce fraudulent refunds by $25 million with an investment of $8 million in staffing and technology. Our actual results confirmed more than $88 million of attempted refund fraud identified **and stopped $42 million attributable directly to this identity screening tool.** [3]

For more information about our successes in Indiana, please see *The Pew Charitable Trusts* article, "States Turn to Data to Hit Back at Fraudsters": http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/11/20/states-turn-to-data-to-hit-back-at-fraudsters.

Alabama Department of Revenue

LNRS helped Alabama stop a fraudulent refund to an identity thief attempting to steal information from a state tax official. *The Wall Street Journal* reported on the incident in April 2015 article, "Even the Tax Man Has a Taxing Time," online at http://www.wsj.com/articles/even-the-tax-man-has-a-taxing-time-1429135915. It says in part:

Joe Garrett's personal and professional lives converged last month when the Alabama state tax official discovered he had become one of the millions of victims of taxpayer-identity theft.

On March 16, Mr. Garrett, a deputy commissioner at the Alabama Department of Revenue in charge of income-tax fraud prevention, returned home to find a form letter in the mail, from his own agency, asking him to confirm his identity information so the state could release his refund.

He hadn't filed yet, so Mr. Garrett knew the letter was bad news. As it turned out, a thief had stolen his personal information and filed tax returns in his name, claiming thousands of dollars in refunds.

"It seemed like a bad joke," said Mr. Garrett.

Then, Mr. Garrett, 44 years old, realized the crime presented an unusual opportunity. "I wanted to understand what happened to me so I could better protect Alabama taxpayers," he said.

3	**Functional Requirements – Identity Fraud and Detection Services** Provide an overview of your approach to identifying fraudulent identities and how you will meet the functional requirements outlined in Section IV-A of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Proactively identify fraud with a high probability while minimizing false positives. 2. Provide a 'best-known' address for the identity. 3. Provide identity confirmation for primary and secondary identities on a tax return (e.g. primary and spouse). 4. Provide identity confirmation for minors or others listed on a return. 5. Accept electronic return data in a format defined by DOR and transmitted back to DOR at least daily. 6. Process up to 150,000 identity records per day and return the results within 24 hours. 7. Provide a draft service level agreement (SLA) with service level failure penalties associated with Respondent(s) service unavailability, erroneous determinations. Once agreed upon and operational, the Respondent(s) shall provide data to support failure and nonfailure of the assertions of the SLA. 8. Properly sign and encrypt all data transmissions to DOR standards (FIPS 140-2). 9. Classify the identities into at least three risk categories based on the Respondent(s) experience, best practices and DOR input. 10. Provide a reason(s) to support the classification of identities. 11. Provide DOR the capability and support to adjust risk classification thresholds of what constitutes a potentially fraudulent identity. 12. Provide trend analysis reports in accordance with industry best practice. 13. Allow DOR to use the provided data for fraud, enforcement, and other revenue programs.

[3] Mike Alley, Testimony of Mike Alley, Commissioner, Indiana Department of Revenue to the US Senate Committee on Finance, March 12, 2015

Pursuant to the DOR's requests above, LNRS complies as indicated in the table below. Also included in this section are descriptions of our solution's functional requirements.

DOR Request	LNRS Response
1. Proactively identify fraud with a high probability while minimizing false positives.	In near-real time a custom batch process evaluates high value risk elements (i.e. bank information, identity information, IP address information, etc.) from various data sources to produce intelligence that is securely shared and integrated into an automated workflow. Certain components of the custom batch process can be configured. The technology reduces false positives and builds an extremely comprehensive and accurate representation of true identities.
2. Provide a 'best-known' address for the identity.	LNRS always provides best-known addresses for input identities, as well as other "best" information available about that identity (i.e. SSN, name, etc.). Addresses in our database are updated on a daily basis.
3. Provide identity confirmation for primary and secondary identities on a tax return (e.g. primary and spouse).	LNRS can provide verification of the vast majority of identities listed on a tax return using our patented LexID linking algorithms and technology
4. Provide identity confirmation for minors or others listed on a return.	LNRS cannot provide verification of minors listed on a tax return.
5. Accept electronic return data in a format defined by DOR and transmitted back to DOR at least daily.	LNRS accepts electronic return data in various formats, develops output files in less than 24 hours (usually in just a couple hours). The output files are securely transferred to the DOR.
6. Process up to 150,000 identity records per day and return the results within 24 hours.	LNRS can meet these requests easily. Our systems generally accommodates over 270 million transactions per hour – with over 100 million identity proofing transactions daily – and we're equipped to handle much more.
7. Provide a draft service level agreement (SLA) with service level failure penalties associated with Respondent(s) service unavailability, erroneous determinations. Once agreed upon and operational, the Respondent(s) shall provide data to support failure and non-failure of the assertions of the SLA.	LNRS is agreeable to entering into Service Level Agreements (SLAs) for our offerings. SLAs are largely dependent upon our ability to control directly all aspects of the product being delivered. SLAs are based upon standard service levels and may include metrics such as: system availability, transaction response times, customer support response times, training, maintenance windows, etc. LNRS can work with the DOR to develop mutually agreeable SLAs as we move forward in this project.
8. Properly sign and encrypt all data transmissions to DOR standards (FIPS 140-2).	LNRS can use PGP encryption on data transmissions to the DOR. PGP key exchange is necessary to support this functionality.
9. Classify the identities into at least three risk categories based on the Respondent(s) experience, best practices and DOR input.	LNRS will work with the DOR to create as many risk categories as you desire. The common four risk categories are: High, Low, Deceased and Incarcerated.
10. Provide a reason(s) to support the classification of identities.	The detailed output file(s) generated provides a reason(s) to support the classification of identities and is configurable

11. Provide DOR the capability and support to adjust risk classification thresholds of what constitutes a potentially fraudulent identity.	LNRS Fraud Data Analysts and a Batch representative will work with DOR personnel and data to customize the risk classification to best meet your needs. As the tax season progresses, the Fraud Data Analysts and/or Batch will continue to work with the DOR to make any necessary changes in the risk scoring to help better process returns, improve classifying identities and minimize fraud risk as determined by the DOR.
12. Provide trend analysis reports in accordance with industry best practice.	As DOR and other customers input records into the LNRS analytical platform, a viewable history is built over time showing counts, amounts and trends of risky and non-risky tax return data.
13. Allow DOR to use the provided data for fraud, enforcement, and other revenue programs.	The DOR may use the output data and intelligence for fraud, enforcement, and any other revenue programs pursuant to the terms and conditions for access to and use of the provided data and services.

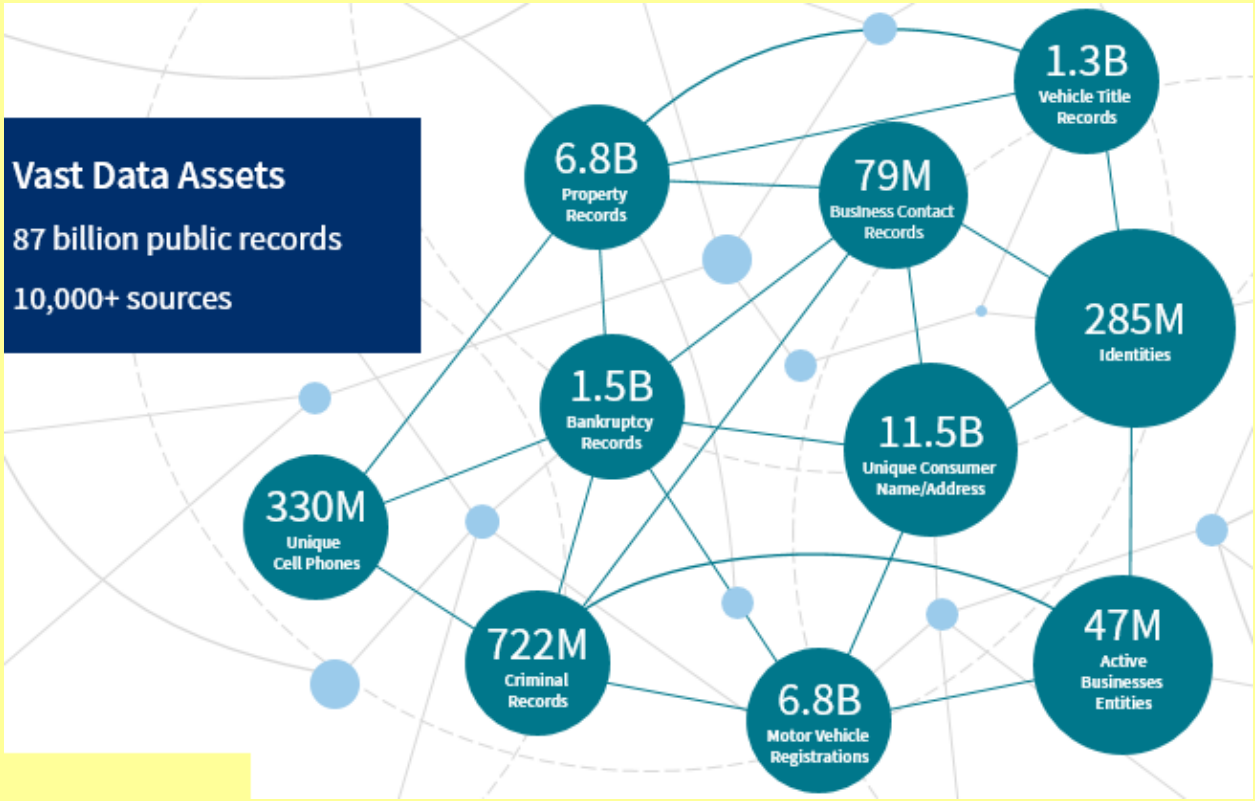
A. Functions and Features

1. Data

No competitive offering matches the expansive LNRS collection of identity data and world class data analytics. While they may claim to incorporate public records data, they typically use a limited number of sources, such as utility and telecommunications data or they draw upon only one bureau's credit data. By contrast, LNRS provides more data (87+ billion public and proprietary records) across **more types of information** and aggregated from **more individual sources** (10,000+) than any other vendor in the world. We take this approach to provide more in-depth insight into individual identities as well as broader insight across the population as a whole.

LNRS gathers its data from public and proprietary sources including federal, state and local entities nationwide. LNRS data comes from all sources the RFP requires and more:

- **All three major credit bureaus**
- Telecommunications and phone data providers (including over 330 million cell phones)
- Property records (6.8 billion)
- Death records (192 million)
- SSNs
- Motor vehicle registrations (6.8 billion)
- Vehicle title records (1.4 billion)
- Vital records
- Utility providers
- Resident services files
- Consumer records
- Arrest and incarceration records
- Drivers licenses
- Professional licenses
- ID cards
- Much more



- LNRS data includes: people, AKAs and alternative names, credit header data from the three major bureaus, relatives & associates, phones (landline, cell, VoIP), addresses & address types, deeds & mortgages, real property assessments, vehicle records, death records, utility and resident service files, Social Security numbers, businesses, voter registrations, email addresses, legal records, assets, derogatory data, employment data, professional licenses, and much more.

RIN leverages the vast data listed above, as well as other data, to analyze efficiently hundreds of unique identity characteristics and identify when there is a possible risk associated to an input tax return. **RIN is also able to ingest and analyze other input data provided by DOR and other RIN customers.** This data includes high value data attributes evaluating risk (list is not all inclusive):

- IP Address
- Bank Account Information
- Preparer Information
- Taxpayer History

These additional data elements are used to ensure that the taxpayer's filing behavior is consistent with the above identity network data elements.

Exclusive data available only through RIN

RIN is the only identity-based refund fraud detection solution that provides and incorporates:

(a) Internet Protocol address metadata
(b) Bank institution data and
(c) Bank account ownership information

- From the input of just the IP address, RIN returns additional information such as the name of the Internet Service Provider (ISP), the physical location associated with the IP address, and the type of connection (proxy, VPN, TOR exit node, etc.) used by the IP address.

- From the bank's routing number, RIN returns additional information such as the bank name, headquarters, type of institution, and whether it has branch offices in the same state as the taxpayer.
- From the bank routing number and taxpayer account number, RIN returns a score indicating the likelihood that the account is actually owned by the taxpayer.

These exclusive pieces of data are vital to understanding the taxpayer's filing behavior and assessing risk of a tax return.

LNRS maintains and hosts a RIN Tax Exchange Database (discussed in detail below) that contains state income tax return information about identities and incidents of alleged tax fraud, material misrepresentation, and serious misconduct related to tax return filings contributed from multiple state tax agencies using the RIN solution.

Within the exchange database, which is near real-time and refreshed daily, states have the ability to query across multiple states data including uniform elements such as: IP address, bank information, taxpayer address, etc. The user has many options for filtering, sorting, wildcard searches and custom queries.

2. Fraud Analysis

The day-to-day fraud risk analysis is accomplished during the automated batch process. DOR will submit newly filed returns to LNRS. The returns are run through RIN, and DOR receives output data, **including a Risk Score**, that becomes the basis for how the return is further processed. The automated batch process is supplemented by the exchange database and use of the Analytic Platform.

Returns that DOR deems to be of low fraud risk continue through the normal return processing. Returns of greater risk, as determined by DOR, have the processing suspended while the taxpayer is required to authenticate further his or her identity using methods available as part of the RIN Solution. The batch processes are explained in greater detail below, while the risk scoring and identity authentication methods are described in this proposal's Sections B and C, respectively.

RIN Workflow Summary

Step in the RIN Workflow	Explanation
Step 1: Taxpayer: Completes and Files Tax Return	In the initial step, the tax filer completes and files a tax return. The proposed solution does not impact the filing process in any way.
Step 2: DOR: Create Input File for LNRS	DOR creates an input file of all submissions received on a daily basis for secure delivery to LNRS. The Input File should be a flat-file, using a delimited format, preferably comma delimited, and include fields such as: Account ID, First Name, Last Name, SSN, Residential Address, and Refund Amount.
Step 3: LNRS: Scan for Risk and Append Attributes	Next, LNRS applies our RIN Solution to review each of the incoming returns for potential fraud. RIN will focus on key areas to validate the filer's identity and assess risk.
Step 4: LNRS: Apply Identity and Return Modeling	LNRS applies patented identity analytics to each refund input and returns a risk score plus other return characteristics.
Step 5: LNRS: Generate Output Files	LNRS develops output files in less than 24 hours, usually in just a couple of hours. The output files are securely transferred to DOR.

Step 6: DOR ingests Output file and Decisions Based on Risk Score	DOR evaluates the return and flags according to risk tolerance
Step 7: Taxpayer Authentication	DOR will notify flagged taxpayers to authenticate themselves in one of two manners: 1. Knowledge based authentication (KBA) 'quiz' that contain questions only the authentic taxpayer should know, but that an identity thief should not. LexisNexis KBA is highly customizable and can include Treasury data if desired. Or 2. Highly configurable one time password (OTP) after a risk assessment on the delivery method (typically via SMS text, but that is also flexible) DOR has the flexibility to give the taxpayer the ability to choose which authentication measure above they want, or deploy a more robust set of risk based criteria only allowing one type of authentication dictated by automated business rules.
Step 8: Taxpayer: Complete authentication (if applicable) / In-Person Investigation with Call-Center	In the event a taxpayer cannot access the Internet, or fails to pass authentication, LNRS recommends the taxpayer be directed to call a DOR customer support to assist them with successfully completing the authentication step.
Step 9: DOR: Unsuccessful authentication process	If a taxpayer cannot resolve the authentication step with the help of the customer support representative, LexisNexis recommends that the return be sent to the designated DOR unit for further review and processing per internal business rules.
Step 10: DOR: Investigates return	N/A

As stated in step 2 above, the RIN process requires DOR to create a file of all tax returns to send securely to LNRS for analysis. LNRS has the capability to transfer securely the flat data files for batch via SFTP using user ID/password authentication. All IDs are whitelisted for IP address as well for additional security. LNRS can also support additional file security by using PGP encryption on the flat data file. PGP key exchange is necessary to support this functionality.

Directly below are the required input/output layouts for the automated batch process of RIN. LNRS recommends the use of delimited files. However, field lengths are provided for customers who require a fixed width layout. We can work with input and output fields as depicted in RFP Attachments M and N.

The RIN Solution is coupled with the Batch and the Risk Defense Platform authentication solutions. It's important to note, RIN is also a solution that is vendor neutral and can be fully integrated into DOR's existing systems. RIN supports data exchange and verification (web based and browser based) and supports via secure data exchange of flat files (csv, xml, text). This allows for LNRS hosted browser-based transactions that may be used in a call center situation (not used as a public site), as well as SOAP and REST API

transactions. LNRS has the capability to securely transfer flat data files for batch via SFTP using user ID/password authentication. All IDs are whitelisted for IP address as well for additional security. LNRS can also support additional file security by using PGP encryption on the flat data file. PGP key exchange is necessary to support this functionality. Another method may be agreed upon by both LNRS and DOR**.**

The batch transfer method is a proven, secure batch file transfer that customers to date have chosen to automate. Files are pulled programmatically from DOR and placed on a secure gateway. All data provided by the customer for batch processing must be submitted over a secure delivery method and returned by LNRS using the same secure method.

LNRS provides multiple options for securing this batch file transfer. The secure delivery options LNRS support include:

- Secure FTP (SSH, SLL, or PGP Encryption)
- FTP-PGP encryption of the file
- Batch Web Gateway (SSL Encryption)

Another method may be agreed upon by both LNRS and DOR**. The customer's inquiry data is never added to the LNRS core database for resale and is destroyed upon successful delivery back to DOR.**

The full LNRS RIN solution (batch, analytics and authentication) can be fully integrated into DOR's integrated tax system. LNRS shall coordinate with the OCIO technical staff and Fast Enterprises staff for full integration.

LNRS has processed millions of customer tax returns with a standard service level agreement (SLA) of 24 hours; however, returns are usually analyzed, modeled, and returned to DOR in just a few hours. RIN analysis creates no delays in servicing tax filers. Lastly, our solution is vendor and platform neutral and requires no additional hardware or software to be installed at DOR.

There is no limit to the number of line items DOR may send LNRS for any given return. In fact, we encourage DOR to send any, and all, line items they would like to visually analyze combined with LNRS data. DOR may send files as frequently as desired. LNRS recommends sending files daily.

RIN Processing of DOR Files

Once DOR's file is received, RIN first uses identity analytics and risk scoring on the return filer to assess the whole identity of the filer and understand differences between non-suspicious tax filers, unusual tax filers, and suspicious ones.

Here are just a few examples of whole identity network analyses RIN performs to identify suspicion or confirm the Trusted Taxpayer:

<u>Validity of the applicant's identity data (Does the identity appear to be fabricated?)</u>

Is the filer:

- Related to someone else living at an address?
- Dead more than two years?
- Incarcerated?
- A fabricated identity, or just a recent immigrant or very young?
- A synthetic identity?

Is the address:

- Residential?
- Complete with a legitimate apartment unit designator?
- A prison?
- A transient commercial location such as a hotel, campground, or mail drop, etc.?
- Used by a disproportionate number of identities?
- Is the ZIP code restricted for use as a corporate PO Box only?

Is the SSN:

- Issued?
- Have a valid format?
- Belong to a deceased person?
- Appear to have been issued prior to the applicant's date of birth?
- Used by multiple individuals?

<u>Suspicious or contradictory identity verification (Is there evidence of identity theft or move-in fraud?)</u>

- Does it appear that the true owner of the SSN resides elsewhere?
- Do utility listings and property records contradict the residence claims on the application?
- Does it appear that the true owner of the identity recently moved to a different state?
- Does it appear to be a fabricated identity?

In addition, the following data attributes of the input tax return are evaluated by RIN for risk (list is not all inclusive):

- IP addresses
- ISP
- IP location
- Bank and Bank location
- Likelihood that taxpayer owns the input bank account
- Tax preparer
- Geo-triangulation (relationship between location of address, IP and bank)

RIN is the only solution that provides and incorporates (a) internet address metadata, (b) bank institution data and (c) bank account ownership information. While this data is not strictly information related to an individual's identity, it is **critical** to assessing effectively and efficiently the risk of an incoming tax return.

- Understanding information about the IP address used can show if the filer is using a service that is in the same location and whether the taxpayer is trying to remain anonymous by using a proxy server or the TOR network.
- Understanding bank information can show if the taxpayer is using an institution that has locations in the area where the taxpayer lives.
- Checking the account ownership reveals whether the taxpayer even owns the account to which the funds are being directed.

If any of these three elements are not consistent with the expected behavior of a typical taxpayer, the risk of fraud increases.

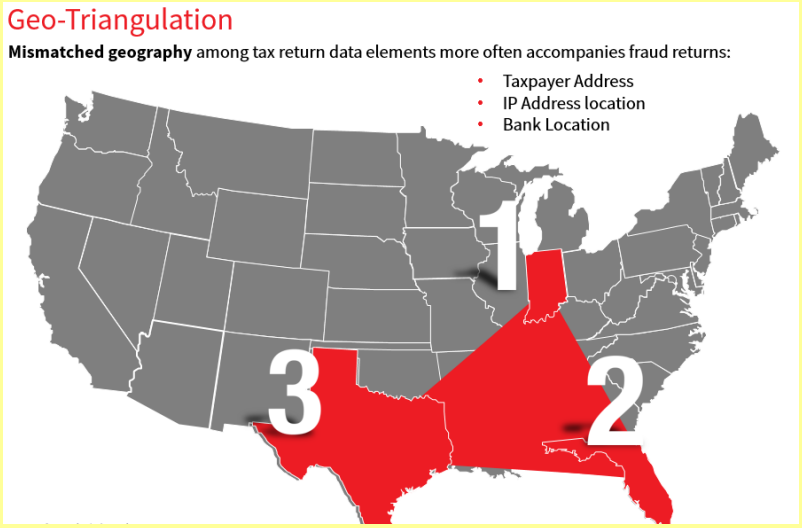
Geo-Triangulation – Exclusive to RIN

Geo-Triangulation is mismatched geography among tax return data elements and more often accompanies fraud returns. Geo-Triangulation is a combination of the following factors:

- IP address location
- Bank location
- Taxpayer address

RIN will programmatically assess the risk associated to, "why is the taxpayer address in Indiana, the IP address location in Miami, Florida and the bank in Texas?" This risk assessment is referred to as, **Geo-Triangulation**, and an even stronger indication of fraud risk, but can also be used to expedite legitimate refund requests.

Geo-Triangulation is exclusive to RIN and is the only solution to provide this metadata.



These exclusive data elements are stored and can be analyzed, either just within DOR's data, via the RIN Visual Analytic Platform (see below on this page) or by incorporating in the Tax Exchange Database (see farther down in this proposal). This analysis can be used to find patterns of use – such as certain ISPs or banks used by fraudsters – and when the patterns are found, quickly incorporating that information into the RIN flagging logic to highlight and stop later filed returns that match those patterns.

RIN has ability to do all of the following:

- Detect and display multiple tax returns from the same source.
- Simultaneously analyze several sets of returns, taxpayers, and associated information.
- Search across all returns in a filing season to identify patterns and schemes that are indicative of fraud.
- Help identify risky bank Wire/Check/ACH and other third-party refund cards financial schemes. LNRS can determine which companies provided the cards.
- Process IRS provided fraud and E-file (MeF) data to identify risks.

Unlike system integrators and vendors without our analytics experience and vast data repository, we have learned how discrepancies in identity that may appear suspicious may not be worth flagging. In addition, we have learned firsthand how integrator and modeler solutions often cannot tell the difference between fraud and a false positive, so they just pass both.

RIN: Visual Analytic Platform

As part of the RIN Solution, non-PII data from the RIN batch output is visually displayed in a user friendly, web based analytical platform and is used for deep-dive analysis by DOR employees tasked with mitigating income tax fraud. This valuable data is posted in near real time and is designed specifically for income tax-based fraud research. Our analytic platform can be deployed across multiple divisions within DOR; it has no user volume limitations.

The visual analytical platform displays both input and output batch data from the jurisdiction's RIN process data, as well as quiz authentication results and is refreshed within 24 hours of the submission of a new file. Users can customize how their data displays via "configurations" that can be saved, changed, and shared with other users. Our state-of-the-art visual analytical platform has no limit on the number of customized configurations and can process millions of records in mere seconds. Additionally, it allows users to save unlimited filtered searches as well as enabling automatically emailed alerts when new data meets those saved searches. As with the configurations, users are able to share high value searches with other users to increase efficiency and distribute workload appropriately.

Contributory E... SELECT CONFIGURATION 100 returns shown of 1,332 returns KY 1 SELECT WE

Processed Date	Orig Refund	Refund	Refund Amount Risk	Std Return Status	Initiate ISP of Interest	Initiate ISP	Initiate Address
08/07/2018	$951.00	$951.00	0	confirmed fraud	0		
08/06/2018	$30,738.00	$30,738.00	1	confirmed fraud	0		
08/01/2018	$882.00	$882.00	0	confirmed fraud	0		
07/25/2018	$199.00	$199.00	0	confirmed fraud	0	att mobility llc	107.77.202.56
07/24/2018	$0.00	$728.00	0	confirmed fraud	0		
07/17/2018	$10,642.00	$10,642.00	1	confirmed fraud	0		
07/13/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
07/11/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
07/10/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
07/09/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		

Above: Partial data view

The robust visual analytic platform, in conjunction with the sophisticated batch output includes, but is not limited to, the following features and functions:

- Detect and display multiple tax returns from the same source
- Simultaneously analyze several sets of returns, taxpayers and associated data
- Search across all returns in a filing season, as well as prior filing seasons, to identify patterns and schemes that are indicative of fraud
- Build and deploy customized fraud and analytics models across multiple divisions within DOR
- Process other data provided to help assess DOR risks
- Identify suspicious bank and bank accounts and other third party refund products
- Export up to 10 million records to Excel
- Model and score to predict future volumes

Our RIN analytic platform can be deployed across multiple divisions. The different user dashboards, screens and functionality will help DOR effectively manage fraud based workloads. Individual taxpayers are identified by our patented LNRS LexID, which can be used in our online Accurint for Government solution to investigate thoroughly and efficiently.

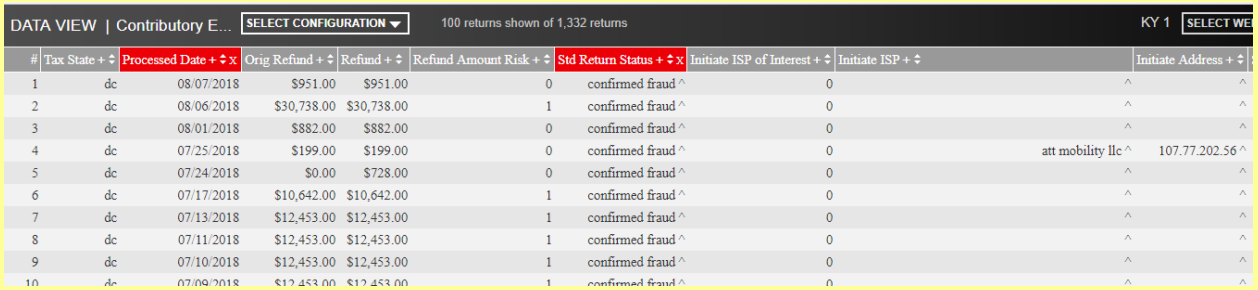
Investigators can use the high-level output information to detect suspicious patterns and trends, and drill down to individual RIN identity records. This allows investigators to combine DOR data and LNRS tax return

risk assessment information and perform ad hoc queries across the agency's return dataset, as well as across other RIN customers' datasets via the Tax Exchange Database.

Some features and function in the visual platform include the following:

Data View

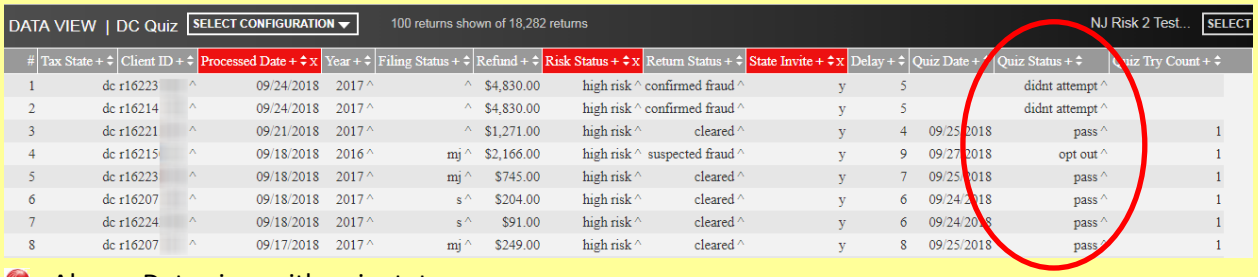
The Data View is the most widely used functionality of the RIN visual analytics platform. This feature gives investigators the ability to customize their view, identity data elements to display, in what order, etc. It supports robust filtering, sorting, wild card searches, saving filters, alerting and processes millions of data in mere seconds to help narrow the scope of investigative research.


DATA VIEW | Contributory E... SELECT CONFIGURATION 100 returns shown of 1,332 returns KY 1 SELECT WE

#	Tax State	Processed Date	Orig Refund	Refund	Refund Amount Risk	Std Return Status	Initiate ISP of Interest	Initiate ISP	Initiate Address
1	dc	08/07/2018	$951.00	$951.00	0	confirmed fraud	0		
2	dc	08/06/2018	$30,738.00	$30,738.00	1	confirmed fraud	0		
3	dc	08/01/2018	$882.00	$882.00	0	confirmed fraud	0		
4	dc	07/25/2018	$199.00	$199.00	0	confirmed fraud	0	att mobility llc	107.77.202.56
5	dc	07/24/2018	$0.00	$728.00	0	confirmed fraud	0		
6	dc	07/17/2018	$10,642.00	$10,642.00	1	confirmed fraud	0		
7	dc	07/13/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
8	dc	07/11/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
9	dc	07/10/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		
10	dc	07/09/2018	$12,453.00	$12,453.00	1	confirmed fraud	0		

- Above: Data view

In the data view, if a return was selected for authentication (i.e. identity quiz), data about the authentication process is tracked and displayed in the visual platform. Data is refreshed daily and elements include the date the quiz was taken and the outcome of the quiz (e.g., pass, fail, didn't attempt or opt out, etc.).

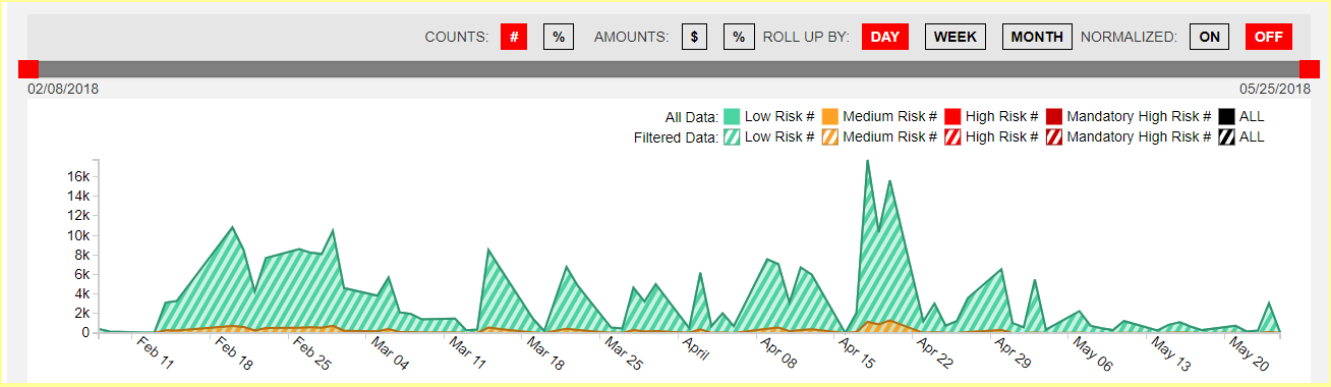

DATA VIEW | DC Quiz SELECT CONFIGURATION 100 returns shown of 18,282 returns NJ Risk 2 Test... SELECT

#	Tax State	Client ID	Processed Date	Year	Filing Status	Refund	Risk Status	Return Status	State Invite	Delay	Quiz Date	Quiz Status	Quiz Try Count
1	dc	r16223	09/24/2018	2017		$4,830.00	high risk	confirmed fraud	y	5		didnt attempt	
2	dc	r16214	09/24/2018	2017		$4,830.00	high risk	confirmed fraud	y	5		didnt attempt	
3	dc	r16221	09/21/2018	2017		$1,271.00	high risk	cleared	y	4	09/25/2018	pass	1
4	dc	r16215	09/18/2018	2016	mj	$2,166.00	high risk	suspected fraud	y	9	09/27/2018	opt out	1
5	dc	r16223	09/18/2018	2017	mj	$745.00	high risk	cleared	y	7	09/25/2018	pass	1
6	dc	r16207	09/18/2018	2017	s	$204.00	high risk	cleared	y	6	09/24/2018	pass	1
7	dc	r16224	09/18/2018	2017	s	$91.00	high risk	cleared	y	6	09/24/2018	pass	1
8	dc	r16207	09/17/2018	2017	mj	$249.00	high risk	cleared	y	8	09/25/2018	pass	1

- Above: Data view with quiz status

Timeseries Chart

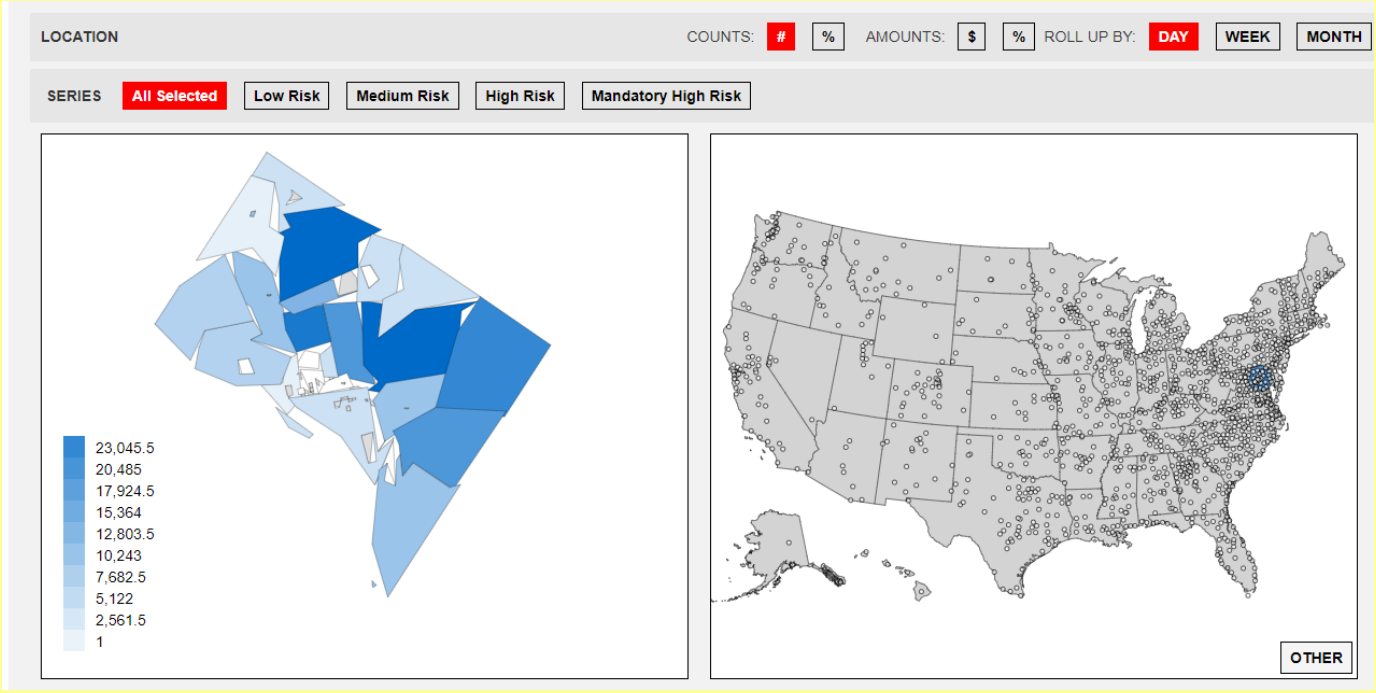
The Timeseries chart is used to show volumes over time and can easily help spot unnatural spikes to the trained eye.



- Above: Timeseries chart view

Maps

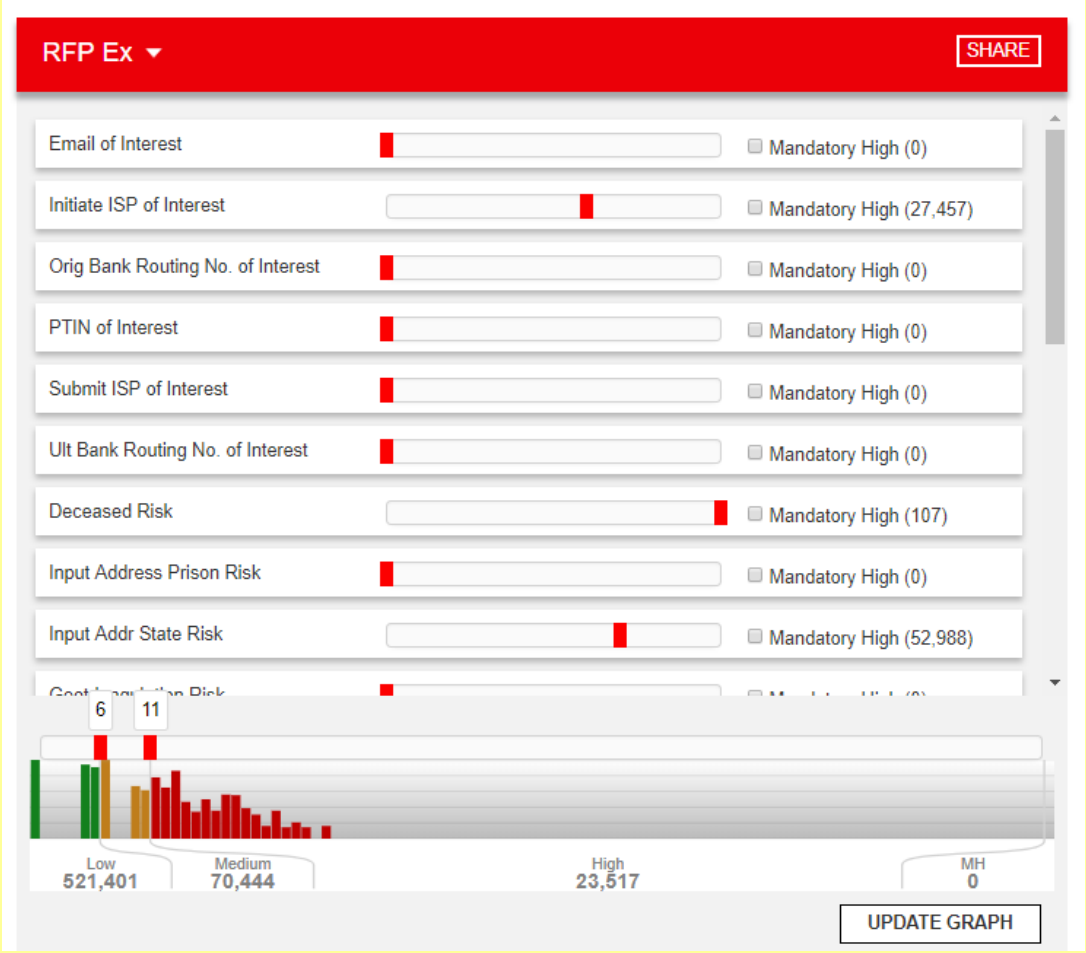
The Maps view is a geospatial view of the customer's jurisdiction broken down by zip codes. There is also a geospatial map of the United States displaying where the return was filed.



- Above: Maps view

Weighting Profiles

The Weighting Profile enables users to easily model changes in risk evaluation to display volumes based on prior data. An unlimited number of customizable weighting profiles can be saved (and shared) per user.



Above: Weighting Profiles view

RIN: Tax Exchange Database

Within the RIN Visual Analytic Platform, DOR users will also have access to RINS's Tax Exchange Database. The database contains state income tax return information about identities and incidents of alleged tax fraud, material misrepresentation, and serious misconduct related to tax return filings contributed from multiple state tax agencies using the RIN solution. The LNRS hosted exchange exclusively for RIN customers, allows members the ability to query across multiple states/agencies in seconds for uniform data elements such as IP addresses, bank information, input addresses, SSN's, LexIDs, etc. in near real-time. The user has many options for filtering, sorting, wildcard searches and custom queries.

High value data elements (contributory) are evaluated routinely by Certified Fraud Analysts across all RIN Exchange customers, which are then used in the automated batch process if associated with increased risk based on adjudicated fraud. This enables the RIN batch to have near real-time inclusion to unique fraud patterns and trends as well as customers leveraging each other's data to help mitigate risk. The following data elements are evaluated for risk in this manner and used by the RIN automated batch process:

- Initiate ISP*
- Submit ISP*
- Original Bank Routing #

- Ultimate Bank Routing #
- Email address
- PTIN

* Derived from input Initiate & Submit IP addresses via our vast IP metadata

RIN returns two output files that contain the contributory data element flags, as well as other risk identified, if present:

- Summary File
- Detailed File

The Summary File is meant to be an "at-a-glance," high-level summary of the risk attributes for easy consumption and decisioning. It contains risk factors such as whether the identity is currently incarcerated, the identity has never been seen at the tax return address, the electronic return was filed from a non-U.S. based location, etc. This file contains approximately 40 output fields.

The Detailed File is a very detailed output file that supports the risk identified in the Summary File, but in much more granular detail. This file also contains customizable "filler" fields where customers can send us certain data points to mirror back to them in our visual analytical platform. This file contains approximately 173 fields.

Global Alerts:

As DOR and other Exchange customers input records into the LNRS analytical platform, a viewable history is built over time showing counts, amounts and trends of risky and non-risky tax return data.

Agencies can launch global alerts that are automatically emailed to users when the saved filter criteria is present in new data, e.g. risky IP addresses, risky bank routing numbers, risky LexIDs, etc. Alerts can be sent daily, weekly or monthly depending on user preference. They can be sent to one or multiple users to help delegate effectively the workload.

3. Online Investigative Research – Accurint for Government

As part of the LNRS solution for DOR, Accurint for Government user licenses are included with unlimited usage. Accurint for Government is a highly useful tool for researching identities beyond the boundaries of RIN identities and DOR data. Accurint for Government is a web site hosted by LNRS that will provide DOR employees unlimited access to perform deep investigations. It also includes free access on mobile devices.

Thousands of government agencies across the country use Accurint for Government to fight fraud, waste and abuse, to enforce laws and regulations, and to provide citizen-centric services. Accurint for Government offers access to billions of public and proprietary records, more than any other provider. With Accurint for Government you can:

- Locate people and discover associations
- Uncover assets
- Investigate businesses
- Visualize complex relationships
- Verify and uncover derogatory information regarding filers

B. Risk Scoring

LNRS data scientists and certified fraud analysts have created a focused, refund fraud-specific model based on many years of mitigating risks effectively for RIN customers. The solution utilizes tax return information to generate a risk score integrating elements such as, but not limited to, taxpayer name, address, SSN, refund amount, IP address and bank account from the input file that DOR provides LNRS.

LNRS will partner closely with DOR's tax experts to analyze past treatment of tax filers and to determine a **custom statistical risk score threshold** that fits DOR's risk tolerance. We will then build that custom risk score into DOR's fraud detection implementation and **trusted taxpayer release patterns**, so it runs natively within the solution in real time. Unlike vendors who only do statistical analysis, we don't need to take DOR's refunds offline to analyze them statistically. We do it in seconds, as the solution runs, with our fraud detection scoring model. The model is built from years of success in many other states fighting identity-based refund fraud. It is tested and updated with new data from the states and other sources daily.

RIN gathers and analyzes hundreds of unique identity characteristics and life events to identify inconsistencies and possible fraud. The RIN risk score goes far beyond pass/fail criteria used to verify if an identity exists and the risk associated. It is a holistic examination into known fraudulent and suspicious profiles using authoritative identity datasets and high-powered analytics. The risk score is derived from more than 200 identity attributes while taking into consideration that all fraud does not look the same. **DOR can customize the risk level** of certain data elements as sometimes rules don't apply or have a different priority within a given state. LNRS knows this from our experience – more experience in refund identity fraud than any other vendor. We also understand this population is unique and the solution must:

- Control for recent moves from one address to another
- Not flag certain classes of people under a certain age
- Compensate for the lack of a Date of Birth or other personally identifiable information (PII) on input
- Understand how spousal identities interact without relying on past assumptions
- Suppress hits for elderly or young identities that show a history at certain kinds of addresses
- Not discriminate against people based on their credit history, tax status or income level
- **Identify the trusted taxpayer**

Finally, one of the most important ingredients in successful fraud detection tax return modeling is incorporating as many different kinds of data into the model as possible in order to determine all risk factors. No other integrator or software vendor has as much success in the government or in Fortune 500 companies as LNRS does in incorporating a wide array of data into models. We leverage our 82 billion records and 735 million unique identities to find predictive factors no integrator or software vendor ever could; **we own, control and link our data**. If a company does not own – but more importantly does not control and link its own data – it lacks a full understanding of the data brought into the company's analytic model.

In addition to identity elements previously described, RIN incorporates and uses a variety of other data elements to develop a risk score that is configured to meet DOR's specific requirements. One such element, **exclusive to LNRS, is our patented High Risk Identifiers (HRI) codes**, which have been developed by LNRS based on the usage of the identity elements in public records and other proprietary information. These codes have been developed by LNRS Predictive Analytic Statisticians working extensively with our data and our customers in various industries over many, many years.

We have identified (and continue to analyze, update, and respond to new fraud behavior) data patterns and trends that successfully predict if an identity is being used by its rightful owner or if there is a risk of misuse, including such situations as use of a stolen or synthetic identity. The RIN solution incorporates those HRI codes that are most predictive of potential identity misuse specifically related to tax refund fraud. We also incorporate, and strongly encourage the use of, additional tax return data elements to be provided by the DOR. These include, but need not be limited to:

- IP Address*
- Bank Account Information*
- Preparer Information
- Taxpayer History
- IRS Fraud Database

* LNRS uses this information to derive additional actionable data including, ISP, IP location, bank location, and likelihood that taxpayer owns the input bank account.

The risk score can be configured in one of two ways. It can either be a numeric score or a category designation, such as "High Risk," "Medium Risk," "Low Risk," etc. LNRS Fraud Analysts will work with DOR personnel and data from DOR to customize the risk score to best meet the needs of the DOR. As the tax season progresses, the LNRS Fraud Analysts will continue to work with DOR to make any necessary changes in the risk score to help DOR better process returns and minimize fraud risk as determined by the DOR.

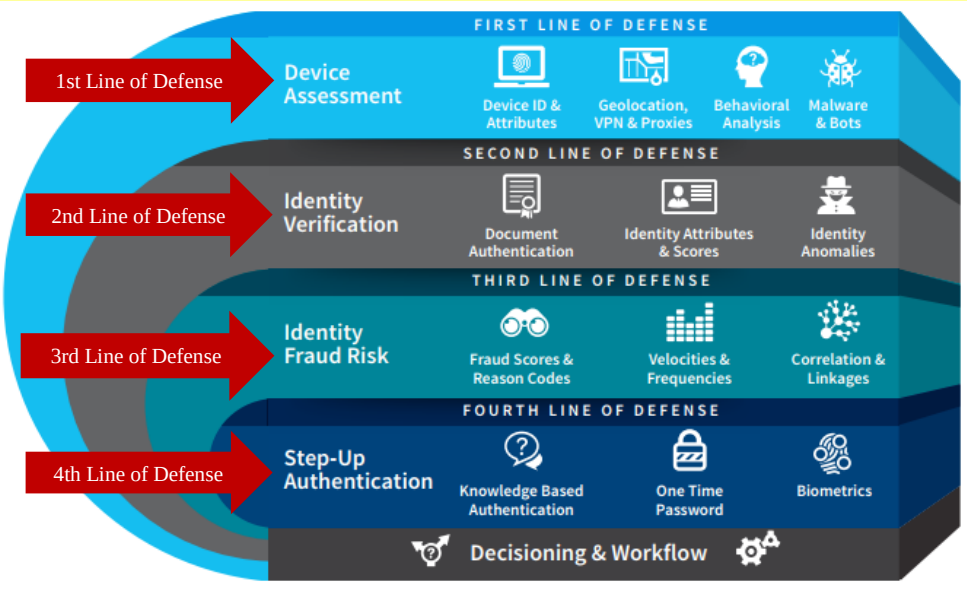
C. Online Portal, Identity Quiz and Authentication Solutions

Identity Proofing with the LNRS Risk Defense Platform

The fraud threat landscape changes direction on a daily basis. Demands for faster, more frictionless citizen interactions are increasing equally as fast. Protecting the DOR with strong levels of fraud prevention and preserving a positive experience for citizens are of paramount importance.

To manage the risk, RIN will seamlessly integrate the LNRS Risk Defense Platform (RDP), a customized risk-based policy decisioning engine that supports your ability to deliver a frictionless identity verification and authentication experience while defending against developing fraud threats.

Through one simplified API integration that requires minimal IT support, RDP delivers seamless access to a myriad of authentication tools and industry-proven decisioning insights that improve your ability to achieve secure authentication and attain the ideal workflow to keep your fraud deflection strategy ahead of the next big threat.



The RDP platform includes sophisticated technologies to address complexities and evolving changes related to verifying identity threats. The RDP suite consists of multiple solutions, with those listed below as a part of this proposal:

- **Identity Verification and InstantID Q&A Quiz (included in this proposal)** authenticates identities of taxpayers, is flexible, and offers more secure questions that do not solely rely on credit bureau information.
- **Phone Finder (included in this proposal)** leverages our 297 million phone numbers and underlying metadata to deliver connections between phones and identities; has a number been forwarded, ported, SIM swapped or other risks.
- **One-Time Password (included in this proposal)** sends alphanumeric authentication code via email, text or voice.

The following are descriptions of three of the RDP verification components offered through this proposal: InstantID Q&A (identity authentication quiz), Ultimate Phone Finder and One Time Password.

InstantID Q&A (Identity Authentication Quiz)

Agencies utilize the LNRS knowledge-based authentication (KBA) quiz to determine whether citizens are who they claim to be.

The InstantID Q&A quiz authenticates an individual based on knowledge of personal information, substantiated by real-time interactive questions and answers. The questions are top-of-mind for your citizens but use unique identity information that is not easily accessible, even for sophisticated fraudsters.
This solution confirms a citizen's identity in seconds by leveraging billions of public records mixed with credit and non-credit data to generate non-intrusive, low-friction authentication questions.

LNRS will work with the DOR to determine flexible user input requirements, such as: last four digits of SSN vs full SSN, answer selection types, response-time velocity, and acceptance/decline criteria. This provides users a superior interactive experience while allowing the DOR to manage, configure and control the authentication risk thresholds.

Ultimate Phone Finder

LexisNexis® Ultimate Phone Finder combines authoritative phone content with the industry's largest repository of identity information to deliver relevant, rank ordered-connections between phones and identities. Gain a clear understanding of the associations between a phone number and an identity to help automate key account activities and support a more efficient account workflow. Ultimate Phone Finder includes approximately 80% of cell phones and Unlisted and Listed landlines

Phone Finder leverages our 297 million phone numbers and underlying metadata to deliver connections between phones and identities; has a number been forwarded, ported, SIM swapped or other risks.

One Time Password

LexisNexis® One Time Password simplifies the authentication process by using devices your customers already have. LexisNexis One Time Password provides a cost effective, easy-to-use alternative, sending a simple alphanumeric authentication code via text or voice to a device they already have in their possession. LexisNexis One Time Password can help protect your system against identity theft, weak passwords,

password reuse, and session-based attacks with little disruption to the customer experience. Additionally, it allows your organization to verify and authenticate users prior to enabling a high-risk or high-value transaction, providing an additional factor of authentication.

D. Integration

The full LNRS RIN solution (batch and authentication) can be fully integrated into DOR's integrated tax system. We will accept your files via mutually acceptable format. Secure delivery options we support include: Secure FTP (SSH, SSL, or PGP Encryption); FTP with PGP encryption of the file; and Batch Web Gateway (SSL Encryption).

The LNRS solution is built using industry standards, such as SOAP and REST. This allows our solutions to communicate and integrate with most any customer system, including FAST Enterprises. As part of our support strategy, we also provide our customers with both a staging area and a production environment. These environments are mutually exclusive and allow for independent testing alongside of the production environment.

As part of our integration strategy, LNRS provides detailed API guides for our online solutions. These include all of the information that is needed to write to our data solutions and all of the options that are required to make the connections.

E. Security

Your peace of mind is our priority. Our customers place their trust in us, and it's a responsibility we take seriously. Because we place a strong, competitive focus on privacy, security and compliance and integrate each of these components into our business model, you can trust that LNRS is a partner who is dedicated to protecting your interests.

Sound privacy, security and compliance practices are essential to the well-being of your agency. We incorporate best practices in these areas into the solutions that we offer customers in business, legal, corporate, government and non-profit organizations.

Mitigating risk for customers and consumers while delivering best-in-class solutions and services is our priority. We strive to employ best-in-industry safeguards so that the information you need is accessible and reliable. Our safeguards are designed to protect you against improper access and impermissible use.

When you choose our solutions, you'll know we are taking steps to help you ensure that your agency and consumer identities are safe, secure and protected. Our risk-management program is designed to provide you with the peace of mind you need to focus on what is most important: driving results for your agency.

4	**Functional Requirements – Identity Investigative Tool for DOR Usage** Provide an overview of your approach to providing an identity investigative tool to DOR and how you will meet the functional requirements outlined in Section IV-B of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement.

	1. Provide an identity investigative tool that is secured to DOR security standards (see Attachment K) for DOR investigative staff to use to research identities. 2. Allow for the ability to discover additional data points around an identity such as potential aliases; other Social Security numbers used; address history; spouse, children, or partner identification; and other unique identifying data points. 3. Provide training to DOR investigative staff on how to use the tool to research identities.

The Accurint for Government online research solution complies with this request.

DOR Request	LNRS Response
1. Provide an identity investigative tool that is secured to DOR security standards (see Attachment K) for DOR investigative staff to use to research identities.	Accurint for Government is an online investigative research solution that is accessible through unique login IDs and passwords for each individual user. LNRS meets and exceeds industry standards for security. LNRS complies with Attachment K pursuant to the attached redlined version of that document.
2. Allow for the ability to discover additional data points around an identity such as potential aliases; other Social Security numbers used; address history; spouse, children, or partner identification; and other unique identifying data points.	LNRS provides all of these data points and more. Please see the summary below for more information.
3. Provide training to DOR investigative staff on how to use the tool to research identities.	LNRS provides all the training that staff members require so they can learn to use the solution effectively and efficiently. Unlimited training is included at no additional charge. We offer training online and onsite from knowledgeable, experienced Education Consultants who understand firsthand the DOR's unique needs.

Online Investigative Research – Accurint for Government

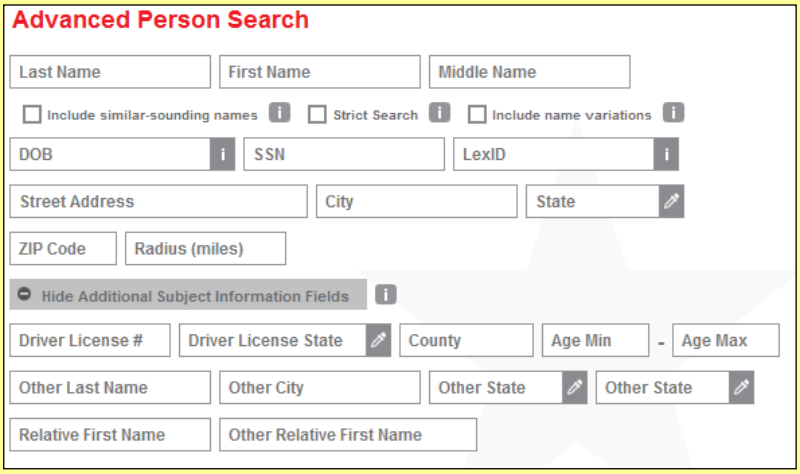
As part of the LNRS solution for DOR, Accurint for Government user licenses are included with unlimited usage. Accurint for Government is a highly useful tool for researching identities beyond the boundaries of RIN identities and DOR data. Accurint for Government is a web site hosted by LNRS that will provide DOR employees unlimited access to perform deep investigations. It also includes free access on mobile devices.

Thousands of government agencies across the country use Accurint for Government to fight fraud, waste and abuse, to enforce laws and regulations, and to provide citizen-centric services. Accurint for Government offers access to billions of public and proprietary records, more than any other provider. With Accurint for Government you can:

- Locate people and discover associations
- Uncover assets
- Investigate businesses
- Visualize complex relationships
- Verify and uncover derogatory information regarding filers

This stand-alone, web-based service can be accessed with a unique user ID and password. Responses are provided within seconds. Special software is not required, and any updates or upgrades are transparent to users. Search results are typically returned in seconds. The Accurint for Government web site is accessible 24 hours a day, 7 days a week.

DOR's Accurint administrators can access usage reports online anytime and have full control to add or delete users as they see fit. We can also provide any usage reports DOR requests on a regular basis or upon request.



Above: Accurint for Government's Advance Person Search Screen. Even if you have partial or missing information about an individual, searching is easy with Accurint form-based searching technology.

Comprehensive Content

- **All 3 credit bureaus**
- **Over 87 billion records**
- **Over 2.5 million new records added daily**
- **Over 285 million unique personal identities with 45 years of data**
- **Over 47 million active (and millions more inactive) business entities**
- **Criminal, incarceration, and sex offense records**
- **Death records**
- **Phones (mobile, prepaid, unlisted)**
- **Utilities (some back to the 1940s)**
- **Real property, motor vehicles, watercraft, and aircraft**
- **Bankruptcies, liens, judgments**
- **Licenses: professional, driving, hunting, fishing, etc.**
- **Marriage, divorce, and civil court records**

Some of the key Accurint for Government search features and functionality available include the following:

- **Advanced Person Search** helps to identify individuals when specific information is not available, or the available information contains errors or is fragmented. The ability to link records based on partial information and to disambiguate and correct errors to create reliable links is a powerful feature only found in Accurint.
- **People at Work Search** - search for records of people connected with businesses to locate your subject and recover revenue and assets. Officers, directors, small business owners and possible employees are just some of the types of records you will find in the People at Work search.
- **Death Records Search** - search death records nationwide.
- **Business Search** - search for a business based on combinations of company name, individual names, federal employer identification number (FEIN), address, city, state, zip, or telephone.
- **Corporate Filings Search** - search for corporate filings based on combinations of company name, officer names, address, city, state, zip.
- **Fictitious Business Name** - search by name, company, address, phone number, or filing number to find what name an entity is doing business as.
- **Federal Employer ID Numbers (FEIN)** - search by company, FEIN, or address to find the FEIN assigned by the Federal Government to business entities expected to file federal tax returns.

- **Bankruptcies, Liens & Judgments Search** - search bankruptcies, tax liens or judgments by name, SSN, LexID, company, FEIN, address, or case number.
- **UCC Filings Search** - search by company name or address to find Uniform Commercial Code (UCC) (commercial lien) filings.
- **FAA Aircraft Search** - search for aircraft registrations based on combinations of names, address, or aircraft number.
- **Motor Vehicle Search** - search for motor vehicle registrations based on combinations of first name, middle name, last name, driver's license number, license plate, company name, SSN, address, city, state, zip.
- **Property (Property Assessments, Deeds & Mortgages)** - search by name, company, address, or parcel number for property tax assessments and property deed records.
- **Watercraft Search** - search commercial and personal craft by name, company, address, hull ID, or vessel name.
- **Driver's License Search** - search driver's license registrations based on combinations of first name, middle name, last name, driver's license number, SSN, LexID, date of birth, address, city, state, zip.
- **Professional Licenses Search** - search by name, social security number, address or professional license number to find individuals that have or have had a professional license.
- **FAA Certifications Search** - search by name or address to find individuals that have or have had pilot, mechanic, trainer, or other FAA certifications.
- **Hunting and Fishing Licenses Search** - search by name, address, or SSN to find individuals that have or have had hunting or fishing licenses.
- **Federal Firearms & Explosives Search** – search by name, address, or license number to find individuals or businesses that have or have had ATF firearms and explosives licenses.
- **Concealed Weapon Permit Search** – search by name, address or SSN to find individuals that have or have had a permit to carry a concealed weapon.
- **DEA Controlled Substances Search** - search by name, address or SSN to find individuals or businesses that have or have had DEA controlled substances licenses.
- **Voter Registration Search** - search by name, address or SSN to find voter registration records.
- **Directory Assistance Search** – search for listed phone numbers based on combinations of first name, middle initial, last name, phone number, address, city, state, zip.
- **Civil Court Records Search** – search by name or address to find civil court records.
- **Official Records Search** - search by name and location for miscellaneous official court filings and other documents.
- **Marriages & Divorces Search** - search marriage and divorce records by name, location, filing number, or LexID.
- **Foreclosures Search** - search foreclosure records by name, company, or address.
- **Link Analysis** - presents relationships between individuals, addresses, vehicles, and corporations. Users expand links dynamically and develop a continuously evolving network of interrelationships.
- **Comprehensive Reports** - creates a combined, comprehensive report compiled from all datasets for either a company or a person.

5	**Functional Requirements – Identity Confirmation** Provide an overview of your approach to providing the capability for individuals to confirm their identity and how you will meet the functional requirements outlined in Section IV-C of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Provide an identity confirmation solution that is question based and that makes the pool of questions available to DOR for selection or adjustment. 2. Provide the ability for DOR to adjust or configure the identity confirmation solution to allow for higher or lower failure rates. 3. Integrate into DOR's pin authentication system for identity confirmation.

DOR Request	LNRS Response
1. Provide an identity confirmation solution that is question based and that makes the pool of questions available to DOR for selection or adjustment.	LNRS uses our own data repository of public, private, and proprietary database sources to dynamically generate up to 70 possible questions – selected by DOR – to increase the probability that only the owner of that identity profile will know the answers. LNRS also allows DOR to submit question changes to LNRS as needed if DOR sees certain questions are not effective or are too difficult to answer. The mix of both historical and current public records data provides additional assurance against fraudulent access due to identity theft. Also, **the quiz is flexible enough to allow for internal proprietary DOR data to be integrated into the quiz.**
2. Provide the ability for DOR to adjust or configure the identity confirmation solution to allow for higher or lower failure rates.	LNRS can customize the questions based on specific DOR requirements, modifying the following variable types: • Number of correct answers required in order to "pass." • Number of attempts an individual has to pass. • Amount of time an individual has to complete the questions. • Types and sources of data to be used. • "Difficulty" of questions. • Ability to deliver "smart" quiz questions based on RIN's batch risk assessment.
3. Integrate into DOR's pin authentication system for identity confirmation.	The solution will comply fully with this request. LNRS designs the online quiz portal to provide a positive, seamless experience for the taxpayer. It will have the same "look and feel" as DOR's system with streamlined login capabilities and seamless access.

Instant ID Q&A (Identity Authentication Quiz)

The LNRS knowledge-based authentication (KBA) quiz determines whether citizens are who they claim to be.

The InstantID Q&A quiz authenticates an individual based on knowledge of personal information, substantiated by real-time interactive questions and answers. The questions are top-of-mind for your citizens but use unique identity information that is not easily accessible, even for sophisticated fraudsters.

This solution confirms a citizen's identity in seconds by leveraging billions of public records mixed with credit and non-credit data to generate non-intrusive, low-friction authentication questions.

LNRS will work with the DOR to determine flexible user input requirements, such as: last four digits of SSN vs full SSN, answer selection types, response-time velocity, and acceptance/decline criteria. This provides users a superior interactive experience while allowing the DOR to manage, configure and control the authentication risk thresholds.

A key differentiator with the LNRS identity proofing solution is that it accesses the "identity network" of every individual. LNRS researches an identity far beyond citizen self-reported input data. To LNRS, an identity consists of a comprehensive network of information going back throughout the history of that identity's rightful owner. To effectively build a network around identities, you must have visibility into individuals in the U.S. legally and illegally. You must also have the linking, fusing, and analytic technology to perform identity resolution on terabytes of data. LNRS has it all.

We offer broad coverage from multiple and dynamic content groups providing an expansive view on citizens' profiles:

- **Consumer Identity –** Credit headers and non-public headers, phone numbers, college information, DOB intelligence, associates, roommates and relatives, voter registrations and drivers' license facts.
- **Residential Sources –** Current and historical address connections, ownership vs. renting, property value, utility service activations, types of address, and address demographics.
- **Owned Assets –** Property ownership, asset value, vehicles, boats and other licensed assets.
- **Business Affiliations –** Corporate registrations, professional licenses and commercial connections.
- **Niche Content Assets –** Shared secrets, customizable internal datasets, identity geo-proximity.
- **And much more.**

To implement the web-based identity authentication, LNRS uses our own data repository of public, private, and proprietary database sources to dynamically generate up to 70 possible questions – selected by DOR – to increase the probability that only the owner of that identity profile will know the answers. LNRS also allows DOR to submit question changes to LNRS as needed if DOR sees certain questions are not effective or are too difficult to answer. The mix of both historical and current public records data provides additional assurance against fraudulent access due to identity theft. Finally, **the quiz is flexible enough to allow for internal proprietary DOR data to be integrated into the quiz.**

During development of the online authentication quiz, DOR may also create its own authentication questions based on internal proprietary DOR data.

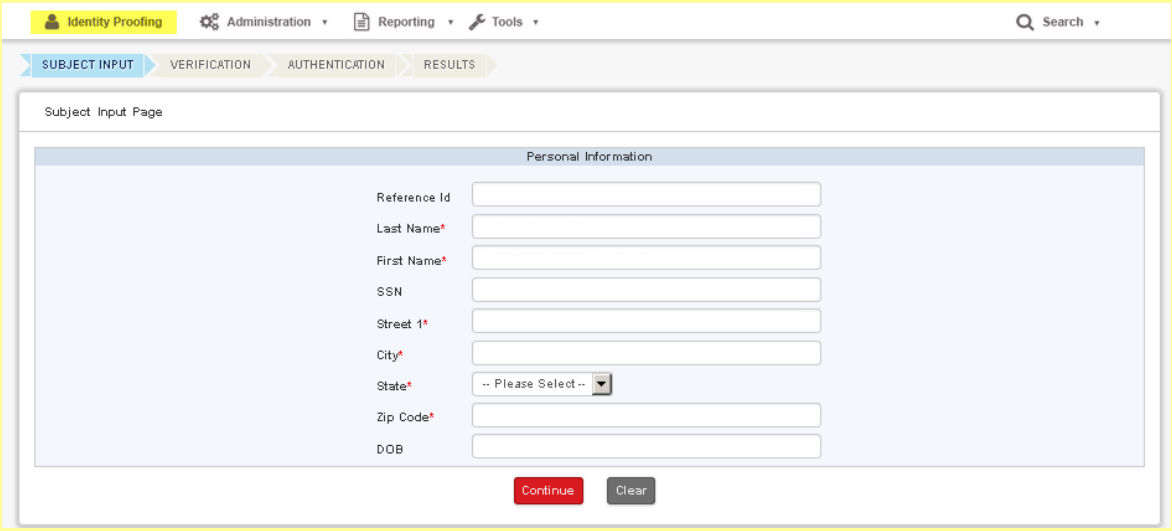
LNRS can customize the questions based on specific DOR requirements, modifying the following variable types:

- Number of correct answers required in order to "pass."
- Number of attempts an individual has to pass.
- Amount of time an individual has to complete the questions.
- Types and sources of data to be used.
- "Difficulty" of questions.
- Ability to deliver "smart" quiz questions based on RIN's batch risk assessment.

For illustration purposes only, the screenshots show steps in the authentication process. **The solution is branded for DOR, not LNRS.**

Step 1

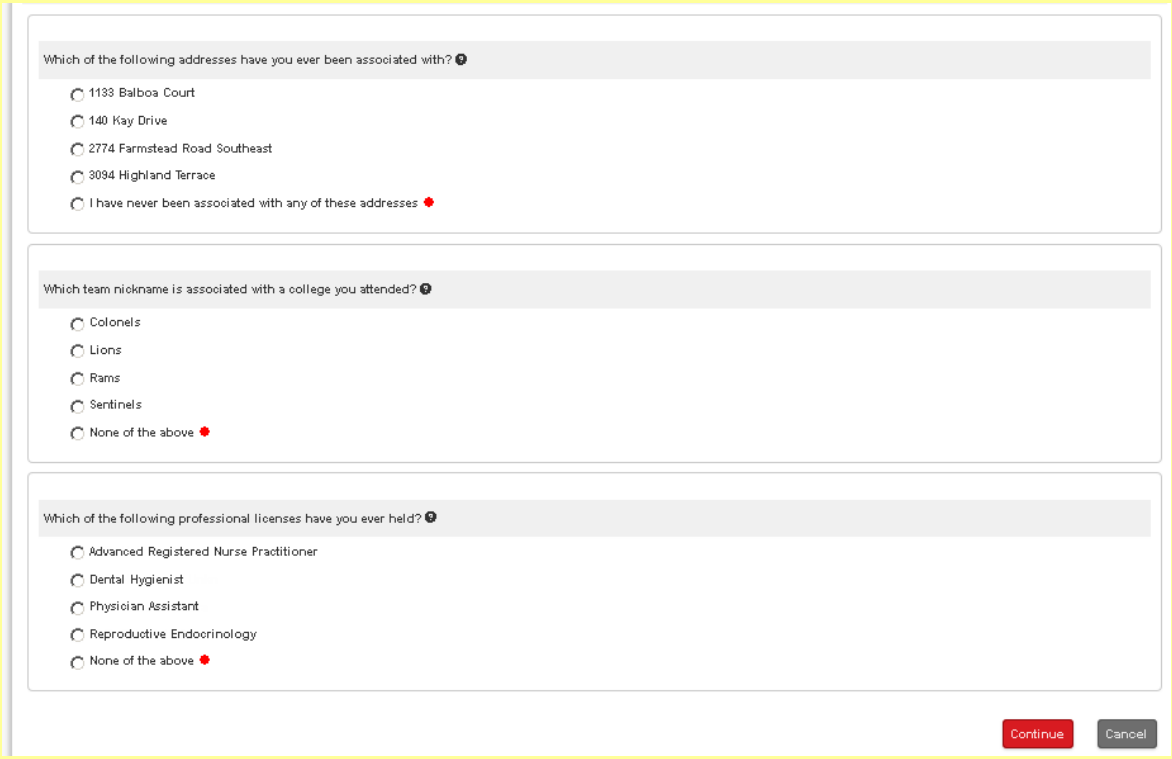
Seamlessly, the tax filer then goes to the DOR web site. The tax filer enters identifying information as determined by the DOR (similar to below). All current LNRS RIN customers require only a unique refund identifier, first and last name, and in some cases last 4 digits of SSN. Fields shown below are for illustration purposes only and do not require the filer to fill in all fields and can be customized as to what the citizen sees.



Above: Online Quiz Step 1.

Step 2

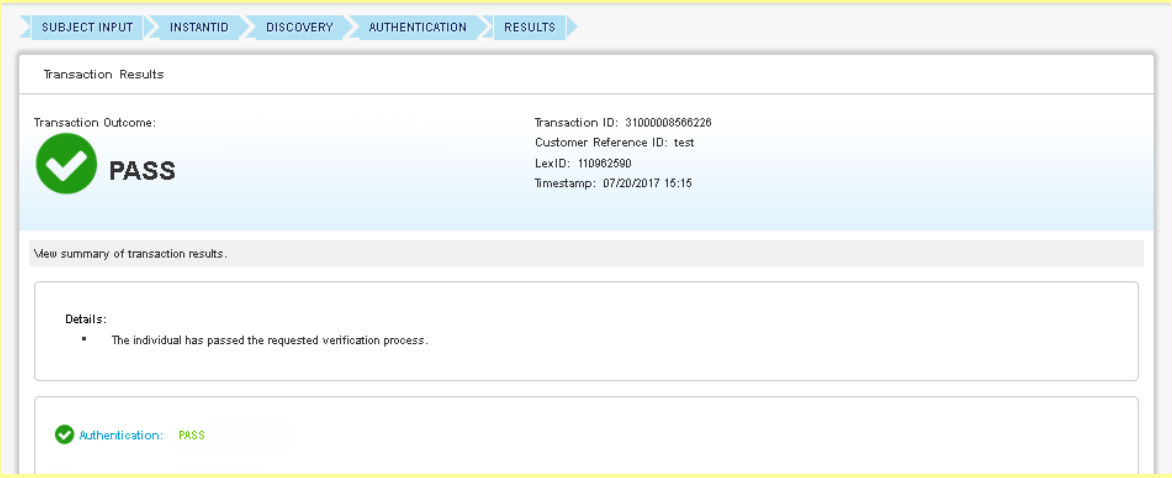
A series of “out of the wallet” questions are generated (below), after Step 1 input is validated.



Above: Online Quiz Step 2.

Step 3

After answering the multiple choice questions, real time authentication results can be presented to the filer if the DOR chooses. LNRS recommends against displaying the status in order to deter criminals from attempting to manipulate the quiz.



Above: Online Quiz Step 3.

Step 4

Lastly, depending on if the identity has passed or failed, DOR will determine if the identity moves through the refund payment process or goes to a manual exception process. The last screen displayed to the citizen, to indicate they have completed the process, will be a custom screen created by DOR.

6	**Functional Requirements – Modeling and Simulation** Provide an overview of your approach to providing modeling and simulation capabilities and how you will meet the functional requirements outlined in Section IV-D of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Provide a simulation tool that enables nontechnical DOR personnel to simulate the effects of fraud rule changes on existing data sets. 2. Provide a simulation environment to test fraud rule changes. 3. Provide a secure simulation environment. 4. Provide training on the proper use of the simulation tool.

LNRS complies with all elements above. Expert statisticians who have modeled data for the largest insurance and banking firms in the world will partner closely with DOR tax experts to analyze past performance and determine a statistical score cutoff that fits your risk threshold. We will then build that into the DOR's implementation, so it runs natively within the solution. As the tax year progresses, LNRS can work with the DOR to adjust those customized scores as the need arises.

An experienced consultant from our Special Investigations Unit (SIU) can also work with the DOR on modeling and simulation. The consultant will experience working for similar state agencies nationwide.

One of the most important ingredients in successful return modeling is incorporating as many different kinds of data into the model as possible in order to find all possible predictive factors. No integrator or software vendor has as much success in the government or Fortune 500 as LNRS does in incorporating a wide array of

data into models. We leverage the billions of records and millions of identities in our database to find predictive factors no one else can.

STLogics – Optional Add On Service

As an optional add-on service, LNRS will partner with subcontractor STLogics for data integration, simulation, modeling support, and training for these services. STLogics possesses deep expertise in modeling and simulation applications for identifying anomalies and performing predictive analytics. The company partners with the DOR now for these purposes.

In addition, the LNRS development approach allows DOR staff to familiarize themselves with the RIN solution on an incremental basis. The approach is used iteratively in the project to develop and test the segments of the solution. For each segment, the same process is followed:

- Batch
- Scoring
- Risk Defense Platform (RDP) assessment, identity verification and authentication workflow
- Analytics
- Reporting

The RIN solution is customized and tested in order to deliver key functionality. Solution and integration testing focuses on meeting user requirements in the areas of usability, functionality, quality, documentation, and performance.

7	**Technical Requirements – Solution Overview** Provide an overview of your solution and how you will meet the functional requirements outlined in Section V-A of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work and identify any issues that you have to fulfill these requirements. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Provide a direct interface with the FAST ITS system to send and receive identities for daily processing. 2. Provide a cloud hosted identity investigation tool supporting all browsers. 3. Encrypt all data at rest and in transit.

DOR Request	LNRS Response
1. Provide a direct interface with the FAST ITS system to send and receive identities for daily processing.	LNRS will interface with the FAST ITS system. We offer a proven, secure file transfer method that is automated. Files are pulled programmatically from DOR and placed on a secure gateway, and LNRS returns files securely using the same method. LNRS has proven history of providing a direct interface with the FAST ITS system with another State DOR to send and receives identity files for daily processing.
2. Provide a cloud hosted identity investigation tool supporting all browsers.	In lieu of cloud hosting, LNRS will host directly within our secure data centers the identity investigative tool. We recommend the following browsers: • Microsoft Edge (Win 10 and higher) • Internet Explorer (IE 11 on Win 7 and higher) • Firefox (Current: 66) • Google Chrome (Current: 73.0.3683.75)

3. Encrypt all data at rest and in transit.	Data is encrypted in transit and at rest. DOR data shall be handled securely, using an approved file format mechanism. We employ industry standards for data encryption and Internet-based secure encrypted file transfer protocols.

The RIN solution can be fully integrated into DOR's integrated tax system. The solution is built using industry standards, such as SOAP and REST. This allows our solutions to communicate and integrate with most any customer system. As part of this support strategy, we also provide our customers with both a staging area and a production environment. These environments are mutually exclusive and allow for independent testing alongside of the production environment.

8	**Technical Requirements – Data Transmission** Provide an overview of your approach to sending and receiving data from DOR and how you will meet the functional requirements outlined in Section V-B of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Accept the State provided identity datapoints similar to those displayed in Attachment M for use in daily identity fraud processing. 2. Deliver datapoints back to DOR daily for investigation use in a format similar to those outlined in Attachment N.

LNRS will accept data points similar to Attachment M and return to the DOR data points similar to Attachment for investigation. We will accept your files via mutually acceptable format. Secure delivery options we support include: Secure FTP (SSH, SSL, or PGP Encryption); FTP with PGP encryption of the file; and Batch Web Gateway (SSL Encryption).

Steps in the RIN Workflow	Explanation
Step 1: Tax Filer: Complete and File Tax Return	In the initial step, the tax filer completes and files a tax return. The proposed solution does not impact the filing process in any way.
Step 2: DOR: Create Input File for LNRS	DOR creates an input file of all submissions received on a daily basis for secure delivery to LNRS. The Input File should be a flat-file, using a delimited format, preferably comma delimited.
Step 3: LNRS: Scan for Risk and Append Attributes	Next, LNRS applies our RIN Solution to review each of the incoming returns for potential fraud. RIN will focus on key areas to validate the filer's identity and assess risk.
Step 4: LNRS: Apply Identity and Return Modeling	LNRS applies patented identity analytics to each return input and returns a risk score plus other return characteristics.
Step 5: LNRS: Generate Output Files	LNRS develops output files in less than 24 hours, usually in just a couple hours. The output files are securely transferred to DOR.
Step 6: DOR: Decisions Based on Risk Score	DOR evaluates the return based on the risk score and determines how return processing proceeds. If there is low risk, it continues through the normal DOR process. If it is higher risk (as defined by DOR), return processing is suspended, and the return moves to Step 7 below.
Step 7: Authentication	DOR will notify flagged tax filers to authenticate their identity via the LNRS Risk Defense Platform.

9	**Technical Requirements – Change Control Process** Provide an overview of your change control process including documentation needed and the terms and conditions surrounding the change control process as identified in Section V-C of the SOW. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement.

The following outlines our change control process:

- A third party ticketing system software is used to manage the change control process.
- Modifications to application systems are tested and evidence of the testing is documented.
- A documented change request is submitted for development and maintenance requests related to the applications.
- Documented change requests are completed for bug fixes, enhancements and new development. Requests are reviewed and prioritized by management teams based on business needs and resource availability.
- Requestor approval forms are required to be submitted whenever the application's appearance, format or data is modified.
- Quality assurance personnel perform testing of code modifications and general application functionality for each submitted change request.
- There is an approval process in place for changes to the production environment.
- Documented policies and procedures are documented to govern the emergency change request process. An emergency change request must be submitted utilizing the third party project management software.
- An emergency publication/business urgency signature form is required to be completed for emergency changes to the production environment. Forms must be signed off by the systems communication specialist and version control specialist.
- A centralized production support group is responsible for migrating changes into production and creating a tracking ticket for each change.
- Only authorized users can make changes.

10	**Technical Requirements – Solution Maintenance** Provide an overview of your approach to the Respondent(s) solution maintenance and how you will meet the functional requirements outlined in Section V-D of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. Provide details on DOR internal support time needed for system upkeep, such as apply monthly OS patches, EOD backups, etc. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Provide scheduled maintenance and emergency releases. 2. Provide software/security patches or releases as needed throughout the year. 3. Provide off-cycle vulnerability patching.

Customers are not required to devote any time for system upkeep. All patching, maintenance, and backups are performed by LNRS.

For maintenance activities, LNRS will failover services to our disaster recovery location while performing the maintenance activities. This ensures that customers are likely not impacted by our maintenance activities. Therefore, the maintenance will be seamless to end users as well as members of the public. LNRS systems maintain 99.9% and greater availability.

LNRS uses a quarterly release cycle for software upgrades. This process has several gates that involve product review and technology review boards. LNRS manages two windows per quarterly release cycles for middleware upgrades and for application upgrades. A third window is coordinated weekly for system

maintenance. This maintenance window is scheduled on Sunday mornings. The three scheduled change windows are as follows:

1. Middleware Upgrades: Wednesdays, 11:00 PM to 3:00 AM ET (once per quarter). The platform utilizes redundant and load balanced infrastructure. Due to our infrastructure, this window does not require an outage.
2. Application Upgrades: Thursdays, 11:00 PM to 3:00AM ET (once per quarter). Our redundant, load balanced infrastructure allows us to maintain system availability during this window.
3. System Maintenance: Sundays, 6:00 AM to 10:00AM ET (once per week). During this time, LNRS performs administrative and operational tasks. In the unlikely event that system changes require down time, customers will receive reasonable advance notice, usually through email.

11	**Technical Requirements – State of Indiana Data** Respondent(s) shall confirm that any data provided by or for the State remains the property of the State and may not be marketed or sold without the express written consent of the State.

LNRS agrees all data provided by the State is the property of the State, and LNRS would not market/sell it without the State's consent. Also, data provided by LNRS from its database is made available to the State pursuant to terms of the LNRS license agreement. The State will receive a limited, non-exclusive, non-transferable license to access and use LNRS data during the contract. Much of the LNRS data is licensed from third parties; therefore, LNRS does not own that data and cannot provide the State ownership of it.

12	**Technical Requirements – Technical Support** Provide an overview of your approach to the Respondent(s) technical support capabilities and how you will meet the functional requirements outlined in Section V-F of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Provide a standard process for problem resolution, including standard response times. 2. Provide an escalation process if the standard resolution process cannot resolve an issue.

LNRS offers 24-hour telephonic support through a toll-free number. For all problems you may also contact your designated Account Manager, Deborah Smith, by phone at (214) 212-5180 or email at Deborah.Smith@lexisnexisrisk.com.

When required, LNRS Customer Support or your Account Manager will escalate an issue to the Tier 1 Technical Team. Tier 1 support includes critical issues that halt or significantly disrupt the LNRS system operations. Tier 1 support will be provided 24 hours per day, seven days per week. LNRS will respond as follows: LNRS will strive to acknowledge receipt of a reported problem within a reasonable time after receiving notification. LNRS will strive to provide follow-up status within a reasonable time after receiving notification. LNRS will provide periodic updates throughout the problem's lifecycle, until all issues are resolved.

When required, the Tier 1 Technical Team will escalate an issue to the Tier 2 Technical Team. Tier 2 support includes troubleshooting important issues that disrupt or interrupt the data exchange between the DOR and the LNRS system. This could include one or more of the following: (1) partial access to the LNRS system or product, (2) partial use of data or functions, (3) reduced performance due to service interruptions, and (4) business operations interrupted. LNRS will respond as follows: LNRS will strive to acknowledge receipt of a reported problem within one hour of receiving notification. LNRS will provide follow-up status within a

reasonable time after receiving notification. LNRS will provide periodic updates throughout the problem's lifecycle, until all issues are resolved.	
13	**Technical Requirements – Disaster Recovery** Provide an overview of your Disaster Recover offering including the ability to provide at least daily backup to DOR as identified in Section V-C of the SOW. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement.
(Confidential – Redacted)	
14	**Staffing: Staffing Plan** Provide an overview of your approach to your staffing plan and how you will meet the functional requirements outlined in Section VI of the SOW. Please describe how your proposed plan and approach will meet each of the functional requirements outlined in the statement of work. The Respondent(s) may propose the same resource as the Account Manager and Implementation Manager if the individual possesses the necessary skills and has the capacity to support both roles. At minimum, confirm your ability to meet the requirement and describe how your plan will fulfill the requirement. 1. Respondent(s) shall provide account management throughout the contract period to support DOR's service and performance requirements. Key activities include: a. Serve as the single point of contact to DOR management. b. Work collaboratively with DOR staff and serve as an escalation point of contact for DOR on inquiries related to account status, system support, account reviews, identity fraud trends and industry best practices. c. Provide initial and ongoing training support. d. Assist DOR to create thresholds and classification definitions as part of the service offering. 2. Respondent(s) shall provide an Implementation Manager from kickoff on January 1, 2021 until the system goes live in September of 2021 to manage the implementation of the fraud detection solution. Key activities include: a. Serve as single point-of-contact to DOR's technical staff during the conversion, implementation and ongoing operations of DOR's fraud services work; b. Manage Respondent(s) implementation work to confirm fulfillment of DOR's testing requirements; c. Have at least three years of experience in an implementation management role (e.g. solution architecture experience); and d. The Implementation Manager may be located at the Respondent(s) location.

Account Management

Deborah Smith shall serve as DOR's designated account manager. She will be the point of contact to DOR management, work collaboratively with DOR staff, and serve as an escalation point of contact for DOR on inquiries related to account status, system support, account reviews, identity fraud trends and industry best practices, and arrange for training. Deborah also will work with other LNRS staff members as needed to assist the DOR with creating thresholds and classification definitions as part of the service offering.

Deborah is a results-oriented Tax Program & Business Development Executive credited with combining program execution, taxation and business development expertise to deliver substantial long-term value for an agency. She has strong expertise in staffing, training and development as well as leveraging in-depth knowledge of tax operations at all levels to meet and state regulations. She is also highly accomplished in strategic planning and ability to build and maintain relationships. Prior to joining LNRS, Deborah served the Ohio Department of Taxation for over 18 years as a Tax Program Executive of Operations and a tax program administer of operations, with Personal Income and Business taxes under her direct purview.

Project and Implementation Management

The DOR's project and implementation manager shall be Monica Brewer. She has implementation, troubleshooting and maintenance responsibilities over all clients utilizing our tax fraud solution as well as other identity authentication and fraud detection services. Monica provides guidance, project plans and communication around the LNRS suite of solutions for the life of the contract for departments of revenue. Her primary goal is to assist the DOR in its effort to combat tax fraud, efficiently process returns of good taxpayers and collaborate across states to detect fraud patterns.

Monica will fulfill duties the DOR requests for implementation support: serve as the single point-of-contact to the DOR's technical staff during conversion, implementation and ongoing operations of DOR's fraud services work; and manage the LNRS implementation and confirm the solution comports with the DOR's testing requirements;

Monica started with our company in 2002 and also has experience in account and sales leadership. She has consistently focused on listening to her customers and placing the highest priority on their satisfaction in their investment in LNRS. Monica earned a Six Sigma yellow belt in an effort to help LNRS and her clients, to identify failing processes, and to make a positive impact in formulating and executing a resolution.

15	**Staffing: Staff Qualifications** Describe how you plan to identify and assign the key personnel required in Section VI of the SOW. Provide the following for each required position: 1. Name and job title; 2. Resume; 3. Employee or subcontractor; 4. Years with company; 5. Location (City and State); 6. Percentage of time committed to DOR; 7. Description of fraud detection experience; 8. Experience with the proposed solution; 9. Description of experiences with a client of similar size and scope to DOR; and 10. Relevant skills, certifications, training and/or experiences

The DOR will work with highly experienced experts in fraud detection and knowledge-based identity authentication. The following are examples of staff member qualifications for individuals who will serve DOR on this project:

- The Account Manager has served previously with the Ohio Department of Taxation for over 18 years as a Tax Program Executive of Operations and a tax program administer of operations, with Personal Income and Business taxes under her direct purview.
- The Senior Fraud Analyst has over 16 years of LNRS experience in tax fraud investigation, and has worked with the DOR from the beginning of the RIN contract.
- The project manager is Six Sigma yellow belt certified and has been with LNRS for 18 years.
- The Batch Consultant has 12 years' experience at LNRS and has served in the data technology sector for over 20 years.
- The Technical Solutions Engineer has over 30 years' experience.

Attached separately are resumes for all key staff members assigned to this project.

16	**DOR Security Standards** Provide an overview of your approach to DOR's security standards and how you will meet the functional requirements outlined in Section VII of the SOW. Please describe how your proposed solution and approach will meet each of the functional requirements outlined in the statement of work. At minimum, confirm your ability to meet the requirement and describe how your solution will fulfill the requirement. 1. Comply with DOR's reading of FISMA, NIST SP800-53 (revision 5), and security best practices found in Attachment K. 2. Comply with FIPS 140-2 Encryption Standard. 3. Comply with DISA STIGs. 4. Provide DOR with a copy of the Respondent(s) technical architecture as part of the RFP response. 5. Conduct a security assessment using the relevant Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) checklists provided by DOR after it reviews the Respondent(s) technical architecture, then provide DOR the results of the STIG checklist prior to orals. Respondent(s) must comply with Category (CAT) 1 checks as prescribed as non-compliance can lead to significant security harm. Respondent(s) should strive to comply with CAT 2 and 3 checks as prescribed. If they cannot comply with checks in those categories, Respondent(s) must provide plans of action and milestones (POA&M) for them, or implement compensating controls. DOR will decide if the POA&Ms and compensating controls are acceptable. 6. Supply evidence of compliance with NIST SP 800-53 and IRS PUB 1075. 7. Manage data security and integrity in the Respondent(s) proposed solution. 8. Certify that the data processed during the performance of this contract will be completely purged from all data storage components of the Respondent(s) computer facility at the end of the calendar year in which the data was received, provided that DOR may extend such period if and solely to the extent such information is retained thereafter in archival form to assist DOR in performing statistical analysis required for DOR's legal or regulatory compliance efforts. 9. Keep all personally identifiable information confidential and secure. 10. In the event of an information disclosure or technical security incident, DOR security must be informed within 24 hours of the incident along with relevant details about: (1) the indications and warnings of compromise were observed; (2) what and when information and systems were potentially compromised; and (3) the mitigating actions taken and planned to protect against and recover from the potential compromise. 11. Inform DOR of subcontractors, partners, and other entities supporting the Respondent(s) in the delivery of services to DOR. Respondent(s) will ensure subcontractors, vendors, and other entities adhere to DOR's security requirements.

Security Overview

LNRS promotes the responsible use of information by employing a risk management framework for privacy, information and physical security, and compliance. The framework is based on ISO 27001/2 and includes administrative, physical, and technical safeguards designed to reasonably protect the privacy, confidentiality, and security of personal information collected from or about consumers. We test our controls within our annual SOC2 Type 2 testing across all five Trust Service Principles (TSPs). As an Identity Proofing Component Member, LNRS has satisfied all requirements for Identity Proofing at the National Institute of Standards in Technology (NIST) Levels 1, 2, and 3 under the Federal Identity, Credential & Access Management (FICAM) Trust Framework Provider 1.0 program. In addition, LNRS is SAFE-BioPharma certified for IAL2.

Proprietary customer credentialing criteria and continuous security controls are also key components of the LNRS privacy, security, and compliance framework. A robust and detailed program of audit and compliance is in constant operation to review and test policies, standards, and guidelines, as well as legal and regulatory requirements, to assess whether they are working effectively and efficiently and being adhered to by customers, employees, and vendors, as appropriate. The LNRS audit program includes in-house and third-party audits as well as independent assessments. Our policies and procedures can be reviewed onsite pursuant to a signed nondisclosure agreement.

LNRS has a centralized and well-documented Compliance and Investigations Department. We also employ in-depth countermeasures like security policies, firewalls, secure networks, data encryption, detailed logging and detection systems. Furthermore, we work with our customers and others in the industry to improve data safeguards and privacy protections. Our security team works to continually refine our data protection processes to ensure the availability, confidentiality, and integrity of data.

Seven key areas differentiate LNRS in privacy, security and compliance:

1. Risk-Mitigation Framework

LNRS promotes the responsible use of information by employing a risk-management framework for privacy, information and physical security, and compliance. The framework is based on ISO 27002 and includes administrative, physical and technical safeguards designed to reasonably protect the privacy, confidentiality and security of personal information collected from or about consumers. Proprietary customer credentialing criteria and continuous security controls are also key components of the LNRS privacy, security and compliance framework.

2. Data Security

To deliver a consistently high standard for data security, LNRS utilizes controls across systems. In addition to utilizing more than 150 internal controls designed to prevent unauthorized access. LNRS conducts back-end suspicious activity monitoring to detect and respond to anomalous account activity. We also work proactively to identify and resolve potential vulnerabilities in our systems.

3. Credentialing

LNRS credentialing and re-credentialing processes verify that access to data is granted to legitimate individuals or entities and for permissible purposes. Our credentialing and re-credentialing processes include: (1) customers, (2) LNRS employees and (3) vendors/third parties. Through these processes, LNRS helps to mitigate the risk of fraud by verifying and re-verifying LNRS employee background information, customer and vendor business credentials and permissible regulatory and legitimate business purposes for accessing information products, systems and data.

4. Policies, Standards and Guidelines
LNRS has implemented strict policies, standards and guidelines throughout the company that govern data access, protection, transport, restriction, retention, deletion and classification for customers, employees and vendors. Policies, standards and guidelines are reviewed and updated regularly – in light of changing legal, regulatory and operational environments, as well as to address new and emerging threats – and communicated to our customers, employees and vendors on an ongoing basis.

5. Audit and Compliance
A robust and detailed program of audit and compliance is in constant operation to review and test policies, standards and guidelines, as well as legal and regulatory requirements, to assess whether they are working effectively and efficiently and being adhered to by customers, employees and vendors, as appropriate. The LNRS audit program includes in-house and third-party audits as well as independent assessments.

6. Accountability
At LNRS, privacy, security and compliance are integrated into the business model. To us, accountability means fulfilling our obligations to customers, consumers, employees, stakeholders and shareholders, specifically including privacy, security and compliance.

7. Training, Communication, Outreach and Transparency
We are committed to keeping both internal and external stakeholders informed and up to date about what LNRS is doing to respect privacy and keep information secure. Employees receive mandatory training with assessment; and customers, employees and vendors are informed of their obligations relating to privacy, security and compliance. Dedicated LNRS personnel are available to assist consumers with general inquiries and requests.

DOR Request	LNRS Response
1. Comply with DOR's reading of FISMA, NIST SP800-53 (revision 5), and security best practices found in Attachment K	For the DOR's consideration, attached separately is a version of Attachment K with LNRS edits and comments.
2. Comply with FIPS 140-2 Encryption Standard.	**(Confidential – Redacted)**
3. Comply with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).	**(Confidential – Redacted)**
4. Provide DOR with a copy of the Respondent(s) technical architecture as part of the RFP response.	LNRS can share architecture information but does not provide copies pursuant to confidentiality and security standards.
5. Conduct a security assessment using the relevant DISA STIG checklists provided by DOR after it reviews the Respondent(s) technical architecture, then provide DOR the results of the STIG checklist prior to orals. Respondent(s) must comply with Category (CAT) 1 checks as prescribed as non-compliance can lead to significant security harm. Respondent(s) should strive to comply with	LNRS agrees to complete assessments supplied to us by the customer. Any remediation activity would be for items mutually agreed upon as posing security risk to customer data.

CAT 2 and 3 checks as prescribed. If they cannot comply with checks in those categories, Respondent(s) must provide plans of action and milestones (POA&M) for them, or implement compensating controls. DOR will decide if the POA&Ms and compensating controls are acceptable.	
6. Supply evidence of compliance with NIST SP 800-53 and IRS PUB 1075.	**(Confidential – Redacted)**
7. Manage data security and integrity in the Respondent(s) proposed solution.	**(Confidential – Redacted)**
8. Certify that the data processed during the performance of this contract will be completely purged from all data storage components of the Respondent(s) computer facility at the end of the calendar year in which the data was received, provided that DOR may extend such period if and solely to the extent such information is retained thereafter in archival form to assist DOR in performing statistical analysis required for DOR's legal or regulatory compliance efforts.	**(Confidential – Redacted)**

	[redacted]
9. Keep all personally identifiable information confidential and secure.	LNRS complies. Please refer to the response in No. 7 above.
10. In the event of an information disclosure or technical security incident, DOR security must be informed within 24 hours of the incident along with relevant details about: (1) the indications and warnings of compromise were observed; (2) what and when information and systems were potentially compromised; and (3) the mitigating actions taken and planned to protect against and recover from the potential compromise.	**(Confidential – Redacted)**
11. Inform DOR of subcontractors, partners, and other entities supporting the Respondent(s) in the delivery of services to DOR. Respondent(s) will ensure subcontractors, vendors, and other entities adhere to DOR's security requirements.	LNRS requires that subcontractors, vendors, and other entities adhere to LNRS security requirements, including those that align with customers' standards.

17	**Project Management Approach** Describe your plan to manage this project from award to implementation as well as provide ongoing services while meeting DOR's requirements and performance standards. At minimum, responses shall: 1. Describe your project management methodology; 2. Provide a draft project plan describing how you plan to implement the processes, staff and technical resources required to meet the requirements of this solicitation both during pre-implementation that will occur between January 2021 – September 2021 and go-live starting in September 2021; 3. Describe your approach to communicating with subcontractor(s) and DOR; 4. Describe your approach to ensuring high quality and timely delivery of contracted services; and Describe your approach to identifying, mitigating and resolving risks and issues.

Upon contract award, LNRS will work with the DOR to identify tasks needed to support the contract and to roll out the solution September 2021 (or another mutually agreeable timeframe if necessary). We can start implementation activities in January 2021 to prevent interference with DOR's filing-season activities. Onsite support will be provided as needed – from the implementation's start date through the life of the contract – to ensure the solution is operating appropriately to ensure all logged tickets are resolved.

The focus of our initial meetings with the DOR will be to learn more about the precise deliverables that the DOR envisions for the fraud detection services. LNRS provides these services today, so much of the groundwork is in place. Representatives from Fast Enterprises should be included in the meeting to establish goals of working collaboratively with LNRS. This input will be critical for us to develop our final project plan.

The output of this initial meeting between LNRS and the DOR will be an implementation plan that (1) outlines the DOR's goals, and (2) provides the service and support to confirm all requirements are satisfactorily achieved. All aspects of our plan will be detailed and reviewed with designated DOR personnel so that established delivery schedules meet your approval. Such approval will be obtained at least one week prior to solution deployment. The plan will be designed as a tool to confirm critical deadlines are met.

From our end, LNRS will assign appropriate resources to ensure our portion of the work is completed within the timeframe both parties agree upon. LNRS will make technical resources available to address questions the DOR may have.

LNRS has a considerable amount of experience with implementation for large agencies, including DOR, and will work diligently with designated contacts to establish service for the DOR. Additionally, the LNRS team will work with each designated DOR point of contact to meet the specific needs within the desired timeframe or other mutually agreed upon schedule.

We can provide a mutually agreeable implementation plan that includes at least the following: installation/configuration details, testing approach, Fast Enterprises integration approach, and a cut-over plan. Our long history of working with the DOR and similar agencies has given us significant knowledge and experience regarding the successful integration and delivery of a solution the DOR desires. As a result, we possess a deep understanding of the complexities involved in the administration of a contract of this size and scope. After the deployment and final signoff, LNRS will begin invoicing for the solution.

Four Phases of Implementation

The LNRS Project Management Methodology has been modeled and influenced by the challenges involved with development initiatives in complex federal, state and local government environments. We have

extensive experience in implementing fraud detection services by leveraging this methodology. The LNRS methodology consists of four phases: Plan, Design, Develop and Deploy.

- **Plan Phase:** Understands, creates, reviews or updates strategic information systems plan and technology.
- **Design Phase:** Creates detailed designs on a project level.
- **Develop Phase:** Uses the detail design documents generated in the design phase to develop and test the system in an iterative process.
- **Deploy Phase:** One or more of the segments are then incorporated into a release that is implemented. Subsequently, additional segments can be incorporated into that release, or second release.

The LNRS Project Management methodology, including analysis, design, and development, encompasses delivering quality services and minimizing risk while meeting the client's business and strategic objectives. LNRS first seeks to fully understand the client's overall vision and then designs, develops and implements a solution that supports the client's business and strategic objectives.

1. Plan Phase

The Plan Phase examines and understands the client's current situation, reviewing documentation, and detailed requirement analysis with a focus on access, reliability, and performance. During this phase, LNRS will conduct Business Process research to establish detailed requirements for the systems, programs and integration with intra- and external business systems.

Sample tasks completed during this phase include:

- Develop strategy to define approaches, processes, and tools based on the technical solution
- Develop solution performance optimization strategy including data, application, hardware, and network considerations
- Define the solution development and deployment strategies to be used
- Develop QA strategy to ensure timely, high-quality delivery
- Develop documentation guidelines
- Develop training strategy to educate staff and enable business users to maximize their use of the solution

2. Design Phase

The Design Phase focuses on defining system requirements within the RIN solution. Deliverables from the Plan Phase are used to support project linkages within the customer's infrastructure. Sample tasks completed during this phase include:

- Define standards and procedures to maximize efficiency of project teams
- Finalize the solution design to optimize the processes for usability and performance
- Complete checkpoints throughout the project to verify milestones are met
- Develop solution design to accurately model the customer's needs based on heavy involvement of the customer through facilitated sessions

3. Development Phase

This iterative approach has the additional benefit of producing results earlier in the project cycle than alternative approaches, allowing state staff to familiarize themselves with the RIN solution on an incremental basis. This phase is used iteratively in the project to develop and test the segments of the solution. For each segment, the same process is followed:

- Batch
- Scoring

- Risk Defense Platform (RDP) device assessment, identity verification and authentication workflow
- Analytics
- Reporting

The RIN solution will be customized and tested in order to deliver key functionality, early. Solution and integration testing focuses on meeting user requirements in the areas of usability, functionality, quality, documentation, and performance.

Sample tasks completed during this phase include:

- Finalize development team requirements
- Solution engineering for hosting and integration with maximum performance and productivity
- Design tests designed to support the metrics defined by the organization
- Solution segments to support continual user feedback

4. Deploy Phase

The Deploy Phase moves the solution into production. To validate before deployment, it is first tested where the deployment plans can be reviewed and system issues can be addressed. The test can then be followed by a general deployment. Prior to Deployment, we will present the DOR with User Acceptance Test results and receive the DOR's approval/signoff.

Sample tasks completed during this phase include:

- Preparation to support the data transfer as needed
- Conversion preparation to help make certain the accurate conversion of the data
- Training for customer staff to help verify the proper use of the solution
- Contingency planning to address issues during deployment
- Disaster recovery environment preparation for rapid recovery
- Deployment reviews to provide feedback for deploying the solution

LNRS staff can be made available as often as needed onsite at DOR premises for the life of the contract to ensure the solution is operating smoothly.

The LNRS team's approach to project management services emphasizes quality throughout the project to ensure the client achieves its overall goals and objectives. We have a proven approach to project management, which includes two key elements:

- Project Management
- Project Monitoring and Control

To ensure RIN is implemented successfully, we will manage at the project level. This will allow us, in conjunction with the client's Project Team, to monitor and maintain complete control of the project from inception to completion.

The LNRS Project Manager will be totally integrated with the client's Project Team, and will coordinate on a daily/weekly/monthly basis. The LNRS Project Management role is principally concerned with the development, design and implementation work, including processes, technical reviews, QA, and task management activities.
Specific Project Management responsibilities are as follows:

- Plan and manage all project resources

- Develop task planning, schedule, performance measurement, and reporting activities
- Ensure that task work planning, scheduling, monitoring, and performance guidelines are followed
- Use internal review processes and preview the project status reports to keep the client apprised of work progress and adherence to established schedule deadlines. Monthly management reviews are completed for quality, performance, financial, and process metrics

In addition, the LNRS Project Management approach follows established policy, and supports tracking and reporting requirements through the status reports and quality assurance reviews. The LNRS Project Management approach implements the following proven management activities into project specific practices:

Requirement Management: The Project Manager first conducts an analysis review of the requirement documents to ensure that the project team has addressed all of the required functions of the RIN solution. If necessary, the project team will produce a gap analysis report that will detail any difference in the requirements and the proposed solution.

Monitor and Track Requirement Changes: Upon approval of the project design specifications, the Project Manager will monitor and track any changes in requirements using the LNRS requirement change request identification and reporting mechanism called a Modify Log. Each change in requirement is identified and input into this Modify Log, and assigned a unique change number linking it back to an original requirement or identifying it as a new requirement.

Sample Implementation Plan

As the DOR's incumbent provider of fraud detection services for over seven years, we remain eager to continue providing all solutions and services. With our solution fully in place at the DOR, you will not lose time and efficiency associated with implementing another vendor's services. You will continue your important work without disruptions and distractions.

Below is a sample implementation plan that we would propose for new setups.

Phase 1 - Plan	**33d**	33d
Contract Paperwork Execution and account(s) set up	30d	30d
Project Implementation kick off and Configuration Review	1d	1d
Deliver Guides and checklists	1d	1d
Schedule ongoing Project Status meetings	1d	1d
Phase 2 - Design	**22d**	22d
LNRS:Customer share layouts	1d	1d
LNRS:Customer design workflow for each use case	10d	10d
LNRS share Staging environment credentials	1d	1d
Complete Data Modeling (as needed)	10d	10d
Phase 3 - Develop & Test	**16d**	16d
Connectivity Test: API and SFTP	1d	1d
LNRS modify and verify Staging Transactions	1d	1d
LNRS provide RDP Reporting Credentials	1d	1d
Training/Overview RDP Reporting Tool	3d	3d
LNRS confirm Data Processing	10d	10d
Phase 4 - Deploy	**12d**	12d
Launch Preparation & Business Readiness	7d	7d
Training (If applicable, may apply to RDP Portal users/Customer Call Center	1d	1d
Provide Production Credentials	1d	1d
LNRS modify and verify Production Transactions	3d	3d
Adjust configuration (if applicable)	0	0
Stakeholder approval	0	0
Go Live!	0	0

- Above: sample implementation for new setups. Because the DOR has already implemented the LNRS solution, many of the steps above do not apply in this case. By choosing LNRS, the DOR will not lose time and efficiency associated with implementing another vendor's services

Data Analysis

LNRS has made substantial financial commitments to ensure that all LNRS Senior Fraud Analysts have the highest qualifications in the area of fraud mitigation. To accomplish this, LNRS' Fraud Analysts have received Certified Fraud Examiner (CFE) certification and have years of experience examining new and emerging fraud patterns. The approach that LNRS takes to data examination is that **identity fraud is always changing and new emerging fraud patterns are always being presented to tax agencies.** This is where the experience of the fraud analyst will benefit the DOR as the LNRS Fraud Analysts work across states and can bring that "wide angle lens" to the DOR. This experience will give the DOR confidence that new patterns can quickly be detected using a combination of RIN Analytics dashboard, the Tax Exchange Database (TED) and the onsite LNRS Fraud Analyst expertise. For example, the LNRS Fraud Analyst will begin to work with the DOR on day one of the contract to employ best practices that have been learned from previous RIN implementations.

Certified Fraud & Forensic Investigations Corp. – Optional Add On Service

LNRS also includes the option to add services of forensic experts who will process the examination and recognition of fraudulent tax returns. We partner with subcontractor Certified Fraud & Forensic Investigations Corp. (CFFI) for this purpose. DOR uses CFFI as part of the DOR's current fraud detection solution. CFFI has extensive experience, evidenced in resumes of CFFI's president and chief operating officer, whose resumes are included in this proposal.

CFFI analyzes risk and assists with identifying fraudulent tax returns. CFFI is a licensed CPA and private investigative firm based in Indianapolis, Indiana. It's made up of anti-fraud experts who specialize in government identity protection solutions. LNRS has enjoyed successful partnership with CFFI for the DOR's existing Fraud Detection Services. CFFI integrates into government agencies to learn and analyze their systems and processes and to implement best practice solutions and on-site leadership for preventing and detecting fraud. CFFI personnel aim to become trusted advisors while providing oversight and making recommendations to enhance the program for maximum fraud-detection results.

18	**Continuous Improvement** Describe your organization's continuous improvement programs and practices. At minimum, responses shall: 1. Describe recent improvements to your company's organization, fraud detection processes and/or technologies; 2. Describe planned improvements to your company's organization, fraud detection processes and/or technologies; 3. Provide your plan to provide ongoing training to DOR to ensure they remain abreast with product updates and trends identified in the industry; 4. Describe how any planned improvements will impact your delivery of services to DOR, and your approach to ensuring successful implementation for DOR; and 5. Provide the timeline for completion of planned improvements.

The LNRS identity risk defense strategy is unparalleled. Our solution suite is the subject of continual evaluation, evolution, and improvement. As recognized by The 2020 Forrester Wave™, we are a global market leader when it comes to our strategy and vision in meeting the ever-changing needs required to combat identity misuse.

LexisNexis Risk Solutions has best-in-class, differentiated execution of its roadmap, coupled with strong leadership and exceptional focus.

-Forrester Wave Report Q2 2020

LNRS switched recently to the RIN platform that we develop to improve our tax identity fraud solution while saving money for the DOR. Advantages of RIN include:
– Link Charts. They allow for evaluating the information used by the identity.
– **Holistic Evaluation.** RIN goes beyond evaluating an independent tax return. It evaluates risk at the identity level.
– Known Risk. RIN flags new tax returns or identities that are re-filed later with the agency.

In the last 24 months, we have evolved and developed new authentication products based on our class-leading repository of identity data. We also have made tremendous investment in the acquisition of solutions that work hand-in-glove with our traditional competencies. With an eye to improving our ability to detect and avoid digital-based identity risk, we have acquired ThreatMetrix, ID Analytics, and Emailage, just to name a few prominent examples.

By choosing LNRS, the DOR will benefit from immediate alignment with the full suite of capabilities that LNRS provides – now and into the future.

Training Plan

LNRS shall provide all the training required for DOR to implement and use effectively the solution and any future improvements/upgrades. Ease of integration, implementation support, ongoing technical support, training, project management, and fraud analytics are all key components to the success of an enterprise fraud detection and identity proofing solution. LNRS has successful experience developing, implementing,

onboarding and supporting scalable identity solutions in federal, state, and local government agencies of all sizes, including DOR.

DOR shall continue to benefit from attentive account management including training for any pre-/post-deployment activities and refresher training as often as you like for your personnel. LNRS production staff, training professionals and technical support will remain fully engaged with DOR to monitor the solution's progress and make recommendations and adjustments to ensure maximum utilization and the overall success of the project.

LNRS agrees to provide system training to all DOR staff. Documentation and training related to maintaining the implemented solution in subsequent filing seasons shall also be provided.

Proposed Training Plan

- Unlimited, hands-on, in-person or remote, computer-based training.
- Utilize "live" DOR data combined with RIN in the analytics dashboard during the training.
- A LNRS Certified Senior Fraud Analyst assigned to the DOR will come onsite or be available for virtual meetings as often as needed for hands on training and data analysis.
- Web and telephonic training sessions are always available as well; however, we prefer to work with DOR employees in person as often as possible.

Length of Training

- One-half day.
- As needed thereafter.

Scope of Training

- Hands-on, computer-based training.
- Requires Internet access.
- Users will conclude training with an in-depth understanding of Accurint for Government and the components of the RIN Analytics Dashboard and Tax Exchange Database (TED):
    - "Risk Assessment" tab to gain an understanding of the volume of refunds being processed nightly, the financial value associated and the ability to query
    - "Identity Authentication" tab to gain an in depth understanding of quiz results (identities passed, failed, sent to quiz, quiz completed, quiz passed, quiz failed, how long it took to take quiz, etc.)
    - "Return Adjudication" tab to gain an understanding of how DOR has treated the returns.
    - "Data View," which houses all taxpayer data that is exchanged with RIN, with no PII being displayed, for in depth investigator analysis.
- Simulate querying real-life fraud scenarios.

Location of Training

- Onsite at your offices, or virtual as needed or preferred. If onsite, a training room or conference room is preferred with computer and internet access.

19	**Quality Assurance** Describe how you plan to execute quality assurance. At minimum, responses shall: 1. Provide a draft quality management plan describing your proposed approach to quality planning, management, control and reporting; 2. Provide a sample corrective plan used for a previous or current client used to address performance issues; 3. Describe your plan to prevent, identify, document and resolve occurrences of employee and/or subcontractor non-compliance with your standard operating procedures, state and federal law and DOR's requirements; 4. Describe your plan for communicating occurrences of customer complaints and non-compliance; 5. Describe your methods to analyze, utilize and communicate customer feedback; 6. Describe your plan to prevent, identify, document and resolve customer complaints; and 7. Provide the standard response times for issue escalation.

Quality Assurance Overview

We have a fully documented set of policies and procedures regarding development and production lifecycles, quality assurance, as well as change and problem management. The Quality Assurance Department engages early in the process with our internal developers to create quality test plans and cases. We use automated testing tools and regression techniques to ensure high quality solutions, including the use of automated testing and performance tools for each of the involved components.

All of our development is performed over a version tracking system. We implement internal and external code audits to ensure that newly developed code adheres to the highest standards. All production systems are monitored through end-to-end and component level monitoring tools. All production-related problems are tracked in a ticketing system, and root cause analysis are performed for every relevant problem, with high emphasis in lessons learned and feedback towards process improvements.

LNRS maintains three distinct environments to support our product development and client production implementations.

1. **The development environment** is leveraged for the creation of product enhancements in solution display, analytics, functionality and rule creation. This environment is flexible and changes to reflect the iterative nature of development. Access to the development environment is role based determined by job description and responsibility at LNRS.
2. **The test environment** is leveraged by the LNRS Quality Assurance Team for the testing and validation of enhancements to the products. This team performs both functional and performance testing as well as quality assurance and regression testing. The team reviews changes to the LNRS solutions developed in the development environment to identify any design flaws to be addressed prior to sign off for a production deployment. Additionally the test environment supports client-specific implementations to which their data build and solution delivery will be verified by our Quality Assurance Operations Team. This team ensures the integrity of the client's deployment prior to release. Access to the test environment is role-based and determined by job description and responsibility at LNRS
3. **The production environment** supports LNRS customer's access to solutions in a secure and stable environment. The production environment reflects only product functionality that has completed the project life cycle and passed all reviews from the Quality Assurance, Product Management, Market Planning and Operations Team's approvals. In addition to client access, LNRS employee access to the production environment is role based and determined by job description and responsibility at LNRS.

Standards and Procedures to Ensure Accuracy of Data

LNRS acquires public records and non-public information from established, reputable sources in the government and private sectors. LNRS obtains an assurance from each data supplier that the supplier has the legal right to license or sell the data to LNRS.

While maintaining, using or disseminating personally identifiable information, LNRS takes reasonable steps to assure that the data is accurate, complete, and current. However, due to the nature of public records, non-public information or publicly available information, it is reasonable to expect these files to contain some errors. If a record is suspected to be inaccurate, LNRS will:

- Direct individuals to the government and private entities which collect and maintain public records and publicly available information to correct any claimed inaccuracies found in that data
- Direct individuals to consumer reporting agencies where such agency is the source of the information about the individual and where the individual seeks to correct claimed inaccuracies found in that data.

Reasonable steps will be taken to review content supplied to LNRS. These steps include reviewing:

- The supplier's data collection practices and policies
- The supplier's business practices
- The financial condition of the supplier
- The types of data the supplier sells (public record, publicly available or non-public information)

Client Satisfaction and Feedback

Client satisfaction is among our highest priorities. LNRS has a comprehensive, division-wide customer satisfaction measurement system focused on providing exceptional solutions, service and support at every customer interaction. Activities are focused on several strategic areas: customer on-boarding and maintenance, ongoing account management, customer service support, billing and invoicing and the Go-to-Market process. Within these areas each customer touch-point and supportive process is analyzed to identify any gaps that might have a negative client impact. Moreover, when any changes or technology are introduced, we assume the role of client advocate, ensuring that client impact is at the forefront of every consideration.

Client satisfaction is measured through several direct and indirect methodologies. Random client surveys are generated and analyzed on a monthly basis. Further, incoming telephone calls and written correspondence are coded and classified for timely identification of issues and servicing trends. Once identified, issues are addressed through the efforts of cross-functional teams. Metrics and scorecards are implemented at the process level to ensure a defect-free and consistent experience for all clients regardless of product or demographic location.

While timeframes for response and resolution will vary by issue, we treat all matters as important and will work to resolve them as soon as practical. Please see this Technical Proposal's Section 12 for details about our standard escalation procedure.

Our Marketing Research team helps drive customer focus within LNRS by being a strong advocate for the Voice of the Customer, ensuring their needs are the foundation upon which new product, brand, marketing and strategic excellence is achieved. Customers are invited to participate in annual advisory boards, panels and user groups, where industry leaders discuss trends, best practices and ways LNRS can help them achieve operational efficiencies. Additionally, customer insights captured via telephone and online interviews are used to fuel ideas for product development by uncovering content, technology and analytic requirements of a valued solution. LNRS also tracks customer satisfaction, loyalty and advocacy, and its performance against market needs regularly, to maintain a pulse on our customers' needs and to allow us to quickly respond to changing environments and associated needs.

Quality Management Plan and Corrective Action

For details about our quality management and corrective action plans, please see the separately attached Quality Manual. This includes guidelines for preventing, identifying, documenting and resolving occurrences of non-compliance.