Mississippi Department of Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

David C. Johnson, Executive Director

Notice of Intent to Certify Sole Source

To: Interested Parties

From: David C. Johnson

CC: ITS Project Number 47528

Date: November 7, 2023

Re: Sole Source Certification Number 4558 to provide Incarceration Database subscriptions for the Mississippi Division of Medicaid (DOM)

Contact Name: Kelsey Mathews

Contact Phone Number: 601-432-8123

Contact E-mail Address: Kelsey.Mathews@its.ms.gov

Sole Source Certification Award Details

Regarding Information Technology Services (ITS) Sole Source Certification Number 4558 for the Mississippi Division of Medicaid (DOM), please be advised that ITS intends to award West Publishing Corporation dba Thomson Reuters as the sole source provider of Incarceration Database subscriptions through October 31, 2024, in an amount not to exceed $567,852.00. If DOM opts to renew the Incarceration Database subscriptions, this sole source certification shall be valid through October 31, 2026. Please be advised that ITS will determine if additional support are within scope during the certification period and may increase the spending authority accordingly. Should West Publishing Corporation dba Thomson Reuters change their name during this certification period, then ITS will determine if a recertification is necessary. For an explanation regarding Mississippi state law, policy and procedures for sole source procurements, refer to Attachment B: Sole Source Procurement Overview.

Sole Source Criteria

1. The product or services being purchased must perform a function for which no other product or source of services exist:

   West Publishing Corporation's proprietary ID Risk Analytics with Enhanced Incarceration Data Solution (IDRA) is a comprehensive risk scoring solution that compares Medicaid program participant data against billions of data points, including incarceration and booking records, public records, publicly available information, and proprietary data to identify inconsistencies in program participant identity information. The system matches program participants against the entity resolved public and proprietary third-party data and incarceration data, utilizing proprietary analytic processes, and its enhancement/quality control process removes false positives to provide actionable intelligence. Initial single identity

Board Members - Mark E. Henderson, Chair • Thomas A. Wicker, Vice-Chair • Christa L. Alexander • J. Keith Van Camp • Bill Cook
Legislative Advisors - Senator Scott DeLano • Representative Kent McCarty

match, no match, and partial match results are processed through a series of proprietary analytics to detect behavioral applicant/program participant anomalies, (e.g., incarceration, death, out of state address, and address tied to commercial P.O. Box). To conduct this analysis and data matching, IDRA is integrated with Thomson Reuters' entity-resolved public and proprietary investigative data known as CLEAR as well as Thomson Reuters' configurable risk weighting and scoring of CLEAR ID Confirm.

2. The purchaser must be able to show specific business objectives that can be met only through the unique product or services:

   The proposed solution provides an up-to-date list of incarcerated program participants – from 85% of the jail beds nationally, including more than 95% of the jail beds in MS – covering both the Mississippi Department of Corrections (MDOC) and local facilities. The unique enhancement/quality control process inherent in IDRA matches individuals in the program to incarcerated individuals whether upon booking, at a point in time (i.e., 30 days), and upon release. The solution increases efficiency by removing false positives, providing detailed, actionable intelligence in a timely manner and automates notifications in accordance with agency business rules. The proposed solution expands the coverage outside MDOC to local and out of state facilities. It will greatly reduce the amount of time currently spent on following up on state information and dead-end leads.

   IDRA will provide:

   1. **notification of incarceration of program participants upon booking to reduce provider fraud,**
   2. **notification of incarceration at a period in time, i.e., 30 days, to reduce overpayments to coordinated care organizations,**
   3. **notification upon release to improve continuity of care.**

   The program data is also analyzed for risk across the total population to identify attributes that indicate possible fraud and/or identify theft (e.g., 6+ people eligible from the same address, IP address with 5+ program participants, temporary/alias/disposable emails, etc.). All single identity and shared cross-population results within IDRA are displayed via a Results Viewer that triages applicant/program participant risk flags into high-medium-low risk categories, providing actionable information on the applicant/plan participant population.

3. The product or services must be available only from the manufacturer and not through resellers who could submit competitive pricing for the product or services:

   Thomson Reuters is the owner and sole source provider of IDRA. IDRA is the only solution that utilizes entity resolved third-party data and proprietary analytics, supported by a Special Investigations Unit (SIU), to remove false positives in the incarceration data set. Furthermore, IDRA is the only solution that provides a dashboard view that includes program metrics, data visualizations and analytic trends with regard to national incarceration data. CLEAR and associated data products are not licensed to be resold.

Schedule

Task	Date
First Advertisement Date	11/07/23

Second Advertisement Date	11/14/23
Response Deadline From Objectors	11/22/23 at 3:00 P.M. Central Time
Notice of Award/No Award Posted	Not before 11/23/23

Project Details

DOM needs to more efficiently monitor if and when beneficiaries become incarcerated in order to suspend payments in a timely manner to prevent overpayments and to allow DOM to efficiently reinstate newly released beneficiaries back on Medicaid in order for them to get the care they need. Many of these former inmates have prescriptions for lifesaving drugs and need immediate access to pharmacies. Based on DOM's review of other products, only Thomson Reuters' proprietary algorithm provides significant time and cost savings via significant reduction of false positives.

Submission Instructions and Format of Response from Objecting Parties

Interested parties who have reason to believe that the Incarceration Database subscriptions should not be certified as a sole source should provide information in the following format for the state to use in determining whether or not to proceed with awarding the Sole Source contract to West Publishing Corporation dba Thomson Reuters.

1.1 Interested Party Information

1.1.1 Contact Name, Phone Number and email address

1.1.2 Company Website URL, if applicable

1.2 Objection to Sole Source Certification

1.2.1 Interested parties must present specific objections to the Sole Source certification using the criteria listed above.

1.2.2 A statement regarding the Interested Party's capabilities as related to this Sole Source Certification Request.

1.3 Comments will be accepted at any time prior to Wednesday, November 22, 2023, at 3:00 p.m. (Central Time) to Kelsey Mathews at kelsey.mathews@its.ms.gov or at the Mississippi Department of Information Technology Services, 3771 Eastwood Drive, Jackson, Mississippi 39211. Responses may be delivered by hand, via regular mail, overnight delivery, e-mail or by fax. Fax number is (601) 713-6380. ITS WILL NOT BE RESPONSIBLE FOR DELAYS IN THE DELIVERY OF RESPONSES. It is solely the responsibility of the Interested Parties that responses reach ITS on time. Interested Parties may contact Kelsey Mathews to verify the receipt of their Responses. Responses received after the deadline will be rejected.

1.4 Interested Party responses should include the following information:

SUBMITTED IN RESPONSE TO
Sole Source Certification No. 4558-47528
Accepted until November 22, 2023 @ 3:00 p.m.,
ATTENTION: Kelsey Mathews

If you have any questions concerning the information above or if we can be of further assistance, please contact Kelsey Mathews at 601-432-8123 or via email at kelsey.mathews@its.ms.gov.

Attachment A: Vendor Correspondence
Attachment B: Sole Source Procurement Overview

Attachment A

THOMSON REUTERS®

Eddie Carreras, Director
Thomson Reuters – Government Risk, Fraud & Compliance
610 Opperman Drive
Eagan, MN 55123
Phone: 225-933-8228
eduardo.carreras@tr.com

Jill B. Chastant, CMPA, CPM
IT Procurement Officer | Office of Procurement
Mississippi Division of Medicaid
550 High Street, Suite 1000 | Jackson, MS 39201
Email: Jill.Chastant@medicaid.ms.gov

September 27, 2023

RE: Sole Source Designation—Thomson Reuters ID Risk Analytics with Enhanced Incarceration Data

Dear Ms. Chastant:

Thomson Reuters is pleased to provide you with information regarding our ID Risk Analytics with Enhanced Incarceration Data (IDRA) solution. Thomson Reuters is a market leader in providing government agencies with products that enhance risk management, effectively combat fraud, waste, and abuse, and support serving participants in their programs. This letter confirms that Thomson Reuters is the owner and sole source provider of IDRA.

IDRA is a comprehensive risk scoring solution that compares your Medicaid program participant data against billions of data points, including incarceration and booking records, public records, publicly available information, and proprietary data to identify inconsistencies in program participant identity information. Initial single identity match, no match, and partial match results are processed through a series of proprietary analytics to detect behavioral applicant/program participant anomalies, (e.g., incarceration, death, out of state address, and address tied to commercial P.O. Box). Your program data is also analyzed for risk across the total population to identify attributes that indicate possible fraud and/or identity theft (e.g., 6+ people eligible from the same address, IP addresses with 5+ program participants, temporary/alias/disposable emails, etc.). All single identity and shared cross-population results within IDRA are displayed via a Results Viewer that triages applicant/program participant risk flags into high-medium-low risk categories, providing actionable information on your applicant/plan participant population.

To conduct this robust analysis and data matching, we integrate IDRA with our entity-resolved public and proprietary investigative data known as Thomson Reuters CLEAR (CLEAR). We also integrate our configurable risk weighting and scoring of CLEAR ID Confirm which includes real-time incarceration and arrest data, and proprietary, modeled, and proven behavioral risk analytics. Incarceration data is enhanced by quality assurance, third-party data, and proprietary analytics. IDRA matches program participants to incarceration data, thereby removing false positives in the incarceration data set. IDRA will provide notification of incarceration of program participants at a period in time, i.e., 30 days, to reduce overpayments to your coordinated care organizations as well as notification upon release to improve continuity of care.

THOMSON REUTERS®

As described in more detail in the following sections, no other single product on the market today provides the combination of incarceration data, risk analytics, features, and capabilities as our proprietary IDRA with Enhanced Incarceration Data.

KEY IDENTITY RISK CONTENT (INCLUDING THOMSON REUTERS EXCLUSIVES)

IDRA with Enhanced Incarceration Data is fully integrated with the following content:

- **CLEAR ID Confirm**—CLEAR ID Confirm applies waterfall search technology based on customer parameters to efficiently conduct identity verification on applicants/program participants and to understand the level of validity or risk involved. By comparing user inputs with public and proprietary records, CLEAR ID Confirm resolves identity through field-by-field matching (match/partial match/no match), identity flag hits, and scores, so users readily see whether the identity appears to be valid and which data sources have information on the subject. CLEAR ID Confirm leverages record data from 13 CLEAR contents sets, including the three major Credit Reporting Bureaus (Experian, TransUnion, and Equifax), Bank Account Headers, and proprietary data sets as well as identity flags on death records, multiple Social Security Numbers (SSNs) tied to the same individual, and multiple individuals tied to the same SSN. Verification parameters are fully configurable to customer preferences and risk tolerances.
- **Thomson Reuters CLEAR**—Program investigators are given access to CLEAR, the most comprehensive, online investigative platform that compiles billions of public records, real-time incarceration and arrest records, publicly available information, and proprietary data, for due diligence and investigation.
- **Enhanced Incarceration Records**—IDRA includes gateway access to Appriss' arrest data network, the only real-time network of state and local offender management in existence. This data source is the most comprehensive data network in the country, with more than 160 million incarceration and arrest records, providing access to approximately 85% of the jail beds nationwide, including over 95% of all state and local agencies in MS. This data is enhanced using CLEAR technology and TR analytics for better identity resolution and to eliminate false positives. The data is updated every hour to ensure that the most up-to-date information is available.
- **Real Estate and CMRA Listings**—A proprietary database of online home and Commercial Mail Receiving Agency (CMRA) listings are used to identify fraudulent addresses within IDRA, including, but not limited to UPS Stores, Mail Boxes Etc., Zillow Real Estate, and Rentals. This enhances shared, cross-population analytics and prioritization within the Results Viewer.

ADVANCED FEATURES & CAPABILITIES (INCLUDING THOMSON REUTERS EXCLUSIVES)

In addition to our proprietary data assets, our IDRA with Enhanced Incarceration Data solution includes the following advanced, proprietary analytic features:

- **Individual Applicant/Program Participant Analytics**—Thomson Reuters uses proprietary behavioral analytics developed and maintained by subject matter experts to identify single identity risks based on individual attributes and other anomalies using a 360-degree view of the applicant/program participant. Single identity risk analytics within IDRA provide actionable results which may include, but are not limited to, incarceration length of stay (i.e., 30 days), release of a previously incarcerated program participant, an individual with multiple SSNs, an SSN used by multiple individuals, a temporary/alias/disposable email address, a deceased individual, a mailing address identified as out-of-state, and an address tied to a commercial P.O. Box.

THOMSON REUTERS

- **Shared Applicant/Program Participant Analytics**—Thomson Reuters uses proprietary, modeled, and proven fraud analytics developed and maintained by subject matter experts to identify population risks based on shared applicant/program participant values and other program anomalies using a 360-degree view of the applicant/program participant population. Shared cross population analytics within IDRA provide actionable results, which may include, but are not limited to an email address shared across multiple program participants, sequential/repeating SSN digits, and shared/duplicate IP addresses.
- **Results Viewer**—IDRA with Enhanced Incarceration Data provides a dashboard view that allows users to get an immediate overview of the entire applicant/program participant population and to quickly understand the potential risks associated with the program, including up to 30 Risk Alerts, including incarceration and release status. The Results Viewer includes program metrics, data visualizations, and analytic trends that summarize key attributes and information from multiple sources. Metrics on the results of analytic processing can be filtered to weekly/year-to-date/lifetime statistics by risk category and total benefit dollars associated to prioritize agency resources and to assist with reporting to supervisory organizations. During the onboarding process, program users can configure the dashboard to ensure it focuses on the risk categories and shared attributes that are most relevant to the program. We also can provide support to develop measures for return on investment and savings due to improper payments prevented, as well as measures to demonstrate continuity of care to meet Medicaid program requirements.
- **Risk Alerts**—Risk Alerts provide notifications and are configurable based upon program requirements, giving the agency additional flexibility for different workflows. Risk alert categories include, but are not limited to:
  - Incarcerated program participant – length of stay as per Medicaid program rules
  - Released incarcerated individual, previously suspended
  - CLEAR ID Confirm individual identity score above program thresholds
  - Shared or duplicate addresses, SSNs, emails, and/or phone numbers
  - CMRA address data, both in and out-of-state
  - Duplicate SSN, sequential/repeating SSN digits, or multiple SSNs matching to a single applicant/program participant
  - Deceased applicants/program participants identified in the Social Security Administration's Death Master File
  - Suspicious, disposable, or alias email addresses
- **Special Investigations Unit (SIU) Support**—Thomson Reuters has an in-house SIU comprised of subject matter experts, former state and federal government employees, and former fraud and law enforcement personnel. The SIU reviews all analytic outputs to ensure accuracy and reduce false positives, and continuously monitors for trends and anomalies in program data to identify new fraud schemes and program abuse.

Due to the nature of our data agreements, CLEAR and associated data products are not licensed to be resold.

We would be happy to further discuss with you the exclusive combination of data, analytics, features, and capabilities available within IDRA with Enhanced Incarceration Data. If you have any questions concerning this letter or require additional information, please do not hesitate to contact us.

Sincerely,

Eddie

Eddie Carreras, Director
Government – Risk, Fraud & Compliance
Thomson Reuters

THOMSON REUTERS

The acquisition of information technology for all state agencies and institutions of higher learning (IHLs) is within the scope of the ITS law, found in Mississippi Code Section 25-53-1, et seq., and the policies and procedures established in accordance with this statute, found in the ITS Procurement Handbook posted on the ITS website (www.its.ms.gov).

ITS enabling legislation requires that information technology hardware, software and services be acquired in a manner that insures the maximum of competition among all manufacturers and suppliers of such equipment and services. Accordingly, ITS promotes full and open competition through the issuance of open specifications and the objective evaluation of Interested Party proposals to determine the lowest and best offering to meet an agency's or public university's business requirements. True competition protects the integrity and credibility of purchasing in the public sector and is essential in providing best value and adequate contractual protection for the purchasing entity. In certain limited situations, information technology acquisitions may be sole-sourced.

ITS utilizes the provisions of Public Purchasing Law for Sole Source and Emergency procurements of information technology. Mississippi Public Purchasing Law (Mississippi Code Section 31-7-13) specifies that noncompetitive items available from one source only be exempted from bid requirements (sole-sourced). ITS statute, in Section 25-53-5 (p), permits ITS to utilize provisions in Public Purchasing Law or regulations, when applicable.

Per Public Purchasing law, acquisitions must meet the following criteria to be authorized as sole source:

1. The product or services being purchased must perform a function for which no other product or source of services exists,

2. The purchaser must be able to show specific business objectives that can be met only through the unique product or services, AND

3. The product or services must be available only from the manufacturer and NOT through resellers who could submit competitive pricing for the product or services. The vendor's correspondence regarding this criterion for this project is included as Attachment A.

By policy as documented in the ITS Procurement Handbook, acquisitions of IT services must include the following information to be authorized as sole source:

1. An explanation about why the amount to be expended is reasonable, and

2. An explanation regarding the efforts by the purchaser to obtain the best possible price.

For state agencies, approval of all technology purchases with a lifecycle cost of $5,000 or less, including sole source purchases, has been delegated to the agency. The ITS Procurement Limits Policies for Agencies (a section in the ITS Procurement Handbook) require a minimum of two competitive written bids or proposals for technology purchases with a lifecycle cost over $5,000 but not over $75,000 (not over $25,000 for projects funded by the American Recovery and Reinvestment Act). Since, for single source items, the procuring agency will be unable to obtain two written bids, ITS must certify all sole source acquisitions of information technology with a lifecycle cost greater than $5,000.

Institutions of Higher Learning (IHLs) or public universities have been delegated the authority to certify sole source procurements up to $250,000 lifecycle cost under the ITS Procurement Limits Policies for IHLs (a section in the ITS Procurement Handbook). For the certification of sole source procurements delegated to the CIOs at public universities, the public university must follow ITS' Sole Source Procedure, including advertisement of the intent to award as sole source. Institutions certifying a sole source purchase must ensure the criteria listed above are met and documented in writing by the institution and the Interested Party prior to certifying a product or service as sole source. Sole source documentation must be reviewed and approved by the IHL's CIO for any sole-source certification

above $5,000. All sole source documentation should be retained in the public university's procurement file. Sole source requests above $250,000 lifecycle cost require ITS approval.

Other than the delegations outlined above, all sole source technology procurements must be certified by ITS.

ITS thoroughly reviews Sole Source Certification Requests, determining if competing products and/or services exist. If so, ITS conducts a competitive procurement. If ITS' review confirms the sole source, then a Sole Source advertisement is issued, giving other Interested Parties an opportunity to identify competing products and/or services. Based upon the results of the Sole Source advertisement, ITS will either certify the request as a sole source or conduct a competitive procurement.