STATE OF ILLINOIS
CONTRACT

Illinois Department of Employment Security
Fraud Detection and Case Management Solutions
Contract Number 4100132391

The Parties to this contract are the State of Illinois acting through the undersigned Agency (collectively the State) and the Vendor. This contract, consisting of the signature page and numbered sections listed below and any attachments referenced in this contract, constitute the entire contract between the Parties concerning the subject matter of the contract, and in signing the contract, the Contractor affirms that the Certifications and if applicable the Financial Disclosures and Conflicts of Interest attached hereto are true and accurate as of the date of the Contractor's execution of the contract. This contract supersedes all prior proposals, contracts and understandings between the Parties concerning the subject matter of the contract. This contract can be signed in multiple counterparts upon agreement of the Parties.

Contract includes BidBuy Purchase Order? (The Agency answers this question prior to contract filing.)

x Yes

☐ No

Contract uses Illinois Procurement Gateway Certifications and Disclosures?

☐ Yes (IPG Certifications and Disclosures including FORMS B)

☐ No

1. DESCRIPTION OF SUPPLIES AND SERVICES
2. PRICING
3. TERM AND TERMINATION
4. STANDARD BUSINESS TERMS AND CONDITIONS
5. SUPPLEMENTAL PROVISIONS
6. STANDARD CERTIFICATIONS
7. FINANCIAL DISCLOSURES AND CONFLICTS OF INTEREST (IF APPLICABLE)
8. CONTRACT SPECIFIC CERTIFICATIONS AND DISCLOSURES – "FORMS B" (IF APPLICABLE)
9. PURCHASE ORDER FROM BIDBUY (IF APPLICABLE)

In consideration of the mutual covenants and agreements contained in this contract, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree to the terms and conditions set forth herein and have caused this contract to be executed by their duly authorized representatives on the dates shown on the following CONTRACT SIGNATURES page.

STATE OF ILLINOIS
CONTRACT

Illinois Department of Employment Security
Fraud Detection and Case Management Solutions
Contract Number 4100132391

VENDOR

Vendor Name: Pondera Solutions, LLC, part of Thomson Reuters	Address: 80 Blue Ravine Road, Suite 250 Folsom, CA 95630
Signature: [redacted]	Phone: (703) 628-8703
Printed Name: Sharie A. Kirsch	Fax:
Title: Sr. Vice President	Email: skirsch@ponderasolutions.com
Date: 09/10/20	

STATE OF ILLINOIS

Procuring Agency or University: Illinois Department of Employment Security	Phone:
Street Address: 33 S. State Street; 9th Floor	Fax:
City, State ZIP: Chicago, IL 60603	
Official Signature: [redacted]	Date: 9/11/2020
Printed Name: Kristin A. Richards	
Official's Title: Acting Director	
Legal Signature:	Date:
Legal Printed Name:	
Legal's Title:	
Fiscal Signature:	Date:
Fiscal's Printed Name:	
Fiscal's Title:	

AGENCY USE ONLY NOT PART OF CONTRACTUAL PROVISIONS

- Agency Reference #:
- Project Title: Fraud Detection and Case Management Solutions
- Contract #: 4100132391
- Procurement Method (IFB, RFP, Small Purchase, etc.): COVID-19 Exemption*
- IPB Reference #: N/A
- IPB Publication Date: N/A
- Award Code: N/A
- Subcontractor Utilization? ☐ Yes ☒No Subcontractor Disclosure? ☐ Yes ☒No
- Funding Source:
- Obligation #:
- Small Business Set-Aside? ☐ Yes ☐No Percentage:
- Minority Owned Business? ☐ Yes ☐No Percentage:
- Women Owned Business? ☐ Yes ☐No Percentage:
- Persons with Disabilities Owned Business? ☐ Yes ☐No Percentage:
- Veteran Owned Small Business? ☐ Yes ☐No Percentage:
- Other Preferences?

*** The Gubernatorial Disaster Proclamation issued August 21, 2020 suspends the provisions of the Illinois Procurement Code (30 ILCS 500/) for purchases necessary for response to COVID-19 and other emergency powers as authorized by the Illinois Emergency Management Agency Act (20 ILCS 3305/). In accordance with CPO-GS Notice 2020.05, the Agency entering into this contract has determined that this contract is necessary to respond to COVID-19 and is therefore exempt from the Illinois Procurement Code (30 ILCS 500/) and the Governmental Joint Purchasing Act (30 ILCS517/).**

1. DESCRIPTION OF SUPPLIES AND SERVICES

1.1. BACKGROUND: The Illinois Department of Employment Security (IDES) administers Unemployment Insurance (UI) programs including, but not limited to, the Pandemic Unemployment Assistance (PUA) program created under the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020. Given the unprecedented level of UI and PUA claims filed during the COVID-19 pandemic, additional fraud detection and prevention resources are required to promote and maintain the integrity of the UI programs.

In accordance with the terms and conditions of this Contract, Pondera Solutions LLC ("Pondera" or "Vendor") shall provide the necessary implementation services for the installation and configuration of its fraud analytics (FraudCaster®) and case management (CaseTracker™) solutions (FraudCaster and CaseTracker are collectively referred to as the "System" or "Pondera System"). The Vendor shall render all other services and deliverables described under this Contract including the Attachments. The Vendor certifies that it has the experience and knowledge in performing the work established under this Contract.

1.2. SUPPLIES AND/OR SERVICES REQUIRED: The Parties acknowledge and agree that the following is a high level overview of the services and deliverables that the Vendor shall provide, at a minimum:

1.2.1. The Vendor shall comply with: (i) all applicable federal and state laws, rules, regulations, and other legal authority in the performance of this contract; (ii) the standards and practices of the information technology industry; and (iii) all IDES security procedures, policies, and requirements. Vendor shall obtain at its own expense, all licenses and permissions necessary for the performance of this Contract

1.2.2. The Vendor shall provide the supplies, services, and deliverables identified in the Attachment I (Statement of Work) and Attachment II (Overview of Pondera Fraud Detection & Case Management) which are attached hereto and incorporated into this Contract by reference. The Vendor shall provide the necessary supplies and services for the design, installation, testing, and configuration of the System in accordance with the terms and conditions of this Contract.

1.2.3. The Vendor shall provide IDES with the information necessary to maintain and use the System. Documentation shall include, but is not limited to: (i) operations manual and (ii) training materials.

1.3. PROJECT MANAGEMENT:

1.3.1. Vendor shall manage its staff, keep track of work and work hours and manage issues with any work performance. If there are any issues with the project or Vendor staff, Vendor will, in cooperation with IDES, work to resolve these issues.

1.3.2. The Vendor shall provide clear communications to ensure that IDES has the information required to make educated decisions on the implementation and use of the System.

1.3.3. IDES may require that Vendor report progress and problems (with proposed resolutions), provide records of its performance, participate in scheduled meetings and provide management reports as requested by IDES. Vendor must maintain auditable detail work records to support all charges to IDES.

1.3.4. IDES' Project Manager and the Vendor's Project Manager shall determine an appropriate set of periodic project staff meetings.

1.4. ACCEPTANCE: Upon its submission of a Key Deliverable as identified in Section 2.A of Attachment I (Statement of Work), the Vendor represents that such Deliverable is ready for IDES review. IDES shall have the opportunity to review the Key Deliverables for an Acceptance period of 48-hours from receiving written certification from the Vendor that the Key Deliverable is final and complete. IDES shall provide the Vendor with written notice by the end of the 48-hours review period if the Key Deliverable is acceptable or describe any defects (material nonconformity to the agreed-upon specifications ("defects")) that must be corrected prior to IDES accepting the Key Deliverable. If IDES fails to notify the Vendor within the 48-hour review period, then said Key Deliverable shall be deemed to have been accepted. The Vendor shall correct defects identified by IDES within a period agreed to by the Parties. Following correction of the defects, IDES shall provide the Vendor with written notice of its acceptance or rejection of the Key Deliverable as described in, and within the period in, this Section. The payment of each Key Deliverable is contingent upon acceptance in accordance with this Section. IDES shall accept or reject completion of the Key Deliverable based solely on whether or not there are defects therein and not based on any other factors, including, without limitation, format or style of the Deliverables or the incorporation at that time of additional ideas or functionality.

1.4.1. Go Live: FraudCaster, Case Tracker, and FE Schemes/Network Analyzer will be deemed Accepted when IDES is satisfied that the end-to-end testing has been completed successfully and when the IDES CIO gives written approval to place the Pondera System into production ("Go Live"). The decision whether to Go Live is within IDES' sole discretion. If testing has been successfully completed, IDES CIO's written approval and go-live decision shall not be unreasonably withheld or delayed.

1.5. CONFIDENTIALITY & DATA SECURITY:

1.5.1. The Vendor shall comply with all confidentiality provisions provided under this Contract, including without limitation Attachment B-1 (IDES Supplemental Terms and Conditions), Attachment B-3 (Protection of Social Security Numbers) and Attachment B-4 (Security Requirements for Cloud-Based Technology), which are attached hereto and incorporated into this Contract by reference.

1.5.2. The Vendor is authorized to use the information and data obtained, collected, created, stored or maintained under the Contract for the limited purpose of the performance of this Contract. Any other dissemination or use of the information or data without the express written authority of the IDES Director is specifically prohibited.

1.5.3. The Vendor shall provide a secure physical and cyber environment for the performance of requirements under this Contract. Vendor's physical and cyber security measures shall meet or exceed industry best practices and any standards established under governing laws, regulations, rules, or guidelines, and shall be subject to the review and approval of IDES. Upon written notice from IDES, Vendor shall remedy any security measure deemed inadequate or insufficient by IDES within 15 days, unless circumstances require the remedy on an expedited basis.

1.5.4. Vendor's security controls shall include administrative, technical and physical safeguards that are designed to protect the confidentiality of IDES data. Some of the core features of the Vendor's security controls shall include:

- Policies and standards that govern information technology resources to protect information assets and safeguard personal information;
- Technologies such as firewalls, encryption, endpoint protection, intrusion detection, intrusion prevention, and data loss prevention;
- Ongoing threat and vulnerability assessment and management;
- 24/7 Monitoring of our systems and networks to detect weaknesses and potential intrusions;
- Ongoing mandatory security awareness training program for all employees; and
- Oversight of third parties.

1.5.5. Notwithstanding any other provision of this Contract, the Vendor shall provide notice to the IDES Project Manager as soon as possible within four (4) business hours or twenty-four (24) hours calendar hours, whichever is sooner, following the discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential information ("Security Incident"). Within twenty-four (24) hours of the discovery or reasonable belief of a Security Incident, the Vendor shall provide a written report to the IDES Project Manager detailing the circumstances of the incident as known at the time, which shall include, at a minimum: (1) a description of the nature of the Security Incident; (2) the type of information involved; (3) who may have obtained the information; (4) what steps the Vendor has taken or shall take to investigate the Security Incident; (5) what steps the Vendor has taken or shall take to mitigate any negative effect of the Security Incident; and (6) a point of contact for additional information.

1.5.6. Vendor shall maintain cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data or information transferred to or accessed by the Vendor under or as a result of this Contract.

1.5.7. In accordance with Attachment I (Statement of Work), the Vendor shall develop and deliver a System Security Plan (SSP) to govern this project. The SSP will include information on how data is transported, secured, and purged. It will also describe how data will be used in crossmatches and which Vendor staff will have access to data and for what purpose. The SSP shall be consistent with the confidentiality and data security requirements established under this Contract.

1.6. MILESTONES AND DELIVERABLES: The Vendor shall provide all deliverables in accordance with the project schedule identified in Attachment I (Statement of Work). The Vendor may update the project schedule for deliverables as necessary. Any updates to the project schedule for deliverables must be approved by IDES, provided that IDES' approval shall not be unreasonably withheld.

1.7. VENDOR / STAFF SPECIFICATIONS: The Vendor's staff shall have the knowledge, experience, training, and skill equal to reasonable commercial standards applicable to personnel with similar responsibilities in the business in which Vendor is engaged and shall obtain sufficient knowledge of IDES practices to perform their respective duties and responsibilities under this Contract. At IDES request, the Vendor shall remove any Vendor's staff at any time if the level of technical, business, process, or communications skill is not satisfactory as determined by IDES, in its sole discretion.

1.8. TRANSPORTATION AND DELIVERY: N/A

1.9. SUBCONTRACTING

Subcontractors not allowed.

For purposes of this section, subcontractors are those specifically hired to perform all or part of the work covered by the contract. If subcontractors will be utilized, Vendor must identify below the names and addresses of all subcontractors it will be entering into a contractual agreement that has an annual value of $50,000 or more in the performance of this Contract, together with a description of the work to be performed by the subcontractor and the anticipated amount of money to the extent the information is known that each subcontractor is expected to receive pursuant to the Contract. Attach additional sheets as necessary.

1.9.1. Will subcontractors be utilized? ☐ Yes ☒ No

1.9.2. All contracts with the subcontractors identified above must include the Standard Certifications completed and signed by the subcontractor.

1.9.3. If the annual value of any the subcontracts is more than $50,000, then the Vendor must provide to the State the Financial Disclosures and Conflicts of Interest for that subcontractor.

1.9.4. If the subcontractor is registered in the Illinois Procurement Gateway (IPG) and the Vendor is using the subcontractor's Standard Certifications or Financial Disclosures and Conflicts of Interest from the IPG, then the Vendor must also provide to the State a completed Forms B for the subcontractor.

1.9.5. If at any time during the term of the Contract, Vendor adds or changes any subcontractors, Vendor will be required to promptly notify, in writing, the State Purchasing Officer or the Chief Procurement Officer of the names and addresses and the expected amount of money that each new or replaced subcontractor will receive pursuant to this Contract. Any subcontracts entered into prior to award of the Contract are done at the sole risk of the Vendor and subcontractor(s).

1.10. SUCCESSOR VENDOR

☐ Yes ☒ No This contract is for services subject to 30 ILCS 500/25-80. Heating and air conditioning service contracts, plumbing service contracts, and electrical service contracts are not subject to this requirement. Non-service contracts, construction contracts, qualification based selection contracts, and professional and artistic services contracts are not subject to this requirement.

If yes is checked, then the Vendor certifies:

(i) that it shall offer to assume the collective bargaining obligations of the prior employer, including any existing collective bargaining agreement with the bargaining representative of any existing collective bargaining unit or units performing substantially similar work to the services covered by the contract subject to its bid or offer; and

(ii) that it shall offer employment to all employees currently employed in any existing bargaining unit who perform substantially similar work to the work that will be performed pursuant to this contract.

This certification supersedes a response to certification 4, Form F, of the Illinois Procurement Gateway (IPG).

1.11. WHERE SERVICES ARE TO BE PERFORMED: Unless otherwise disclosed in this section all services shall be performed in the United States. If the Vendor performs the services purchased hereunder in another country in violation of this provision, such action may be deemed by the State as a breach of the contract by Vendor.

Vendor shall disclose the locations where the services required shall be performed and the known or anticipated value of the services to be performed at each location. If the Vendor received additional consideration in the evaluation based on work being performed in the United States, it shall be a breach of contract if the Vendor shifts any such work outside the United States.

- Location where services will be performed: Illinois, California, and Florida

  Value of services performed at this location: 100%

2. PRICING

2.1 TYPE OF PRICING: The Illinois Office of the Comptroller requires the State to indicate whether the contract value is firm or estimated at the time it is submitted for obligation. The total value of this contract is firm.

2.2 EXPENSES ALLOWED: Expenses are not allowed.

2.3 VENDOR'S PRICING: The first-year subscription fee is $656,329 for the Pondera System. In addition, there is a one-time CLEAR data run fee of $198,000.

Payment Milestone	Estimated Invoice Date	Amount
Project Initiation	September 15, 2020	$393,797.40 (60% of the first-year subscription fee)
Delivery of one-time CLEAR batch run of IDES data	September 22, 2020	$198,000 (100% of the one-time data run fee)
FraudCaster & Case Tracker Go-Live:	February 22, 2021	$196,898.70 (30% of the first-year subscription fee)
FE Schemes/Network Analyzer Go-Live:	March 23, 2021	$65,632.90 (10% of the first-year subscription fee)
	Total:	$854,329

2.4.1. Renewal Compensation: If the contract is renewed, the Vendor's annual subscription fee will increase by 3% over the preceding year subscription fee.

2.4 MAXIMUM AMOUNT: The total payments under this contract shall not exceed $854,329 without a formal amendment.

3. TERM AND TERMINATION

3.1 TERM OF THIS CONTRACT: This contract shall commence upon the last dated Signature of the Parties and shall end on September 15, 2021.

3.1.1 In no event will the total term of the contract, including the initial term, any renewal terms and any extensions, exceed 10 years.

3.1.2 Vendor shall not commence billable work in furtherance of the contract prior to final execution of the contract except when permitted pursuant to 30 ILCS 500/20-80.

3.2 RENEWAL: This Contract may be renewed upon mutual written agreement of the Parties. This Contract may neither renew automatically nor renew solely at the Vendor's option. Pricing for the renewal term(s), or the formula for determining price, is shown in the pricing section of this contract.

3.3 TERMINATION FOR CAUSE: The State may terminate this contract, in whole or in part, immediately upon notice to the Vendor if: (a) the State determines that the actions or inactions of the Vendor, its agents, employees or subcontractors have caused, or reasonably could cause, jeopardy to health, safety, or property, or (b) the Vendor has notified the State that it is unable or unwilling to perform the contract.

If Vendor fails to perform to the State's satisfaction any material requirement of this contract, is in violation of a material provision of this contract, or the State determines that the Vendor lacks the financial resources to perform the contract, the State shall provide written notice to the Vendor to cure the problem identified within the period of time specified in the State's written notice. If not cured by that date the State may either: (a) immediately terminate the contract without additional written notice or (b) enforce the terms and conditions of the contract.

For termination due to any of the causes contained in this Section, the State retains its rights to seek any available legal or equitable remedies and damages.

3.4 TERMINATION FOR CONVENIENCE: The State may, for its convenience and with thirty (30) days prior written notice to Vendor, terminate this contract in whole or in part and without payment of any penalty or incurring any further obligation to the Vendor.

3.4.1. Upon submission of invoices and proof of claim, the Vendor shall be entitled to compensation for supplies and services provided in compliance with this contract up to and including the date of termination.

3.5 AVAILABILITY OF APPROPRIATION: This contract is contingent upon and subject to the availability of funds. The State, at its sole option, may terminate or suspend this contract, in whole or in part, without penalty or further payment being required, if (1) the Illinois General Assembly or the federal funding source fails to make an appropriation sufficient to pay such obligation, or if funds needed are insufficient for any reason (30 ILCS 500/20-60), (2) the Governor decreases the Department's funding by reserving some or all of the Department's appropriation(s) pursuant to power delegated to the Governor by the Illinois General Assembly, or (3) the Department determines, in its sole discretion or as directed by the Office of the Governor, that a reduction is necessary or advisable based upon actual or projected

budgetary considerations. Contractor will be notified in writing of the failure of appropriation or of a reduction or decrease.

4. STANDARD BUSINESS TERMS AND CONDITIONS

4.1 PAYMENT TERMS AND CONDITIONS:

4.1.1 Late Payment: Payments, including late payment charges, will be paid in accordance with the State Prompt Payment Act and rules when applicable. 30 ILCS 540; 74 III. Adm. Code 900. This shall be Vendor's sole remedy for late payments by the State. Payment terms contained on Vendor's invoices shall have no force and effect.

4.1.2 Minority Contractor Initiative: Any Vendor awarded a contract under Section 20-10, 20-15, 20-25 or 20-30 of the Illinois Procurement Code (30 ILCS 500) of $1,000 or more is required to pay a fee of $15. The Comptroller shall deduct the fee from the first check issued to the Vendor under the contract and deposit the fee in the Comptroller's Administrative Fund. 15 ILCS 405/23.9.

4.1.3 Expenses: The State will not pay for supplies provided or services rendered, including related expenses, incurred prior to the execution of this contract by the Parties even if the effective date of the contract is prior to execution.

4.1.4 Prevailing Wage: As a condition of receiving payment Vendor must (i) be in compliance with the contract, (ii) pay its employees prevailing wages when required by law, (iii) pay its suppliers and subcontractors according to the terms of their respective contracts, and (iv) provide lien waivers to the State upon request. Examples of prevailing wage categories include public works, printing, janitorial, window washing, building and grounds services, site technician services, natural resource services, security guard and food services. The prevailing wages are revised by the Illinois Department of Labor (DOL) and are available on DOL's official website, which shall be deemed proper notification of any rate changes under this subsection. Vendor is responsible for contacting DOL at 217-782-6206 or (*http://www.state.il.us/agency/idol/index.htm*) to ensure understanding of prevailing wage requirements.

4.1.5 Federal Funding: This contract may be partially or totally funded with Federal funds. If Federal funds are expected to be used, then the percentage of the good/service paid using Federal funds and the total Federal funds expected to be used will be provided to the awarded Vendor in the notice of intent to award.

4.1.6 Invoicing: By submitting an invoice, Vendor certifies that the supplies or services provided meet all requirements of the contract, and the amount billed and expenses incurred are as allowed in the contract. Invoices for supplies purchased, services performed and expenses incurred through June 30 of any year must be submitted to the State no later than July 31 of that year; otherwise Vendor may have to seek payment through the Illinois Court of Claims. 30 ILCS 105/25. All invoices are subject to statutory offset. 30 ILCS 210.

4.1.6.1 Vendor shall not bill for any taxes unless accompanied by proof that the State is subject to the tax. If necessary, Vendor may request the applicable Agency's state tax exemption number and federal tax exemption information.

4.1.6.2 Vendor shall invoice at the completion of this contract unless invoicing is tied in this contract to milestones, deliverables, or other invoicing requirements agreed to in the contract.

Send invoices to:

Agency:	Illinois Department of Employment Security
Attn:	Thomas Revane
Address:	33 South State Street, 11th Floor
City, State Zip	Chicago, Illinois 60603

4.2 ASSIGNMENT: This contract may not be assigned, transferred in whole or in part by Vendor without the prior written consent of the State.

4.3 SUBCONTRACTING: For purposes of this section, subcontractors are those specifically hired to perform all or part of the work covered by the contract. Vendor must receive prior written approval before use of any subcontractors in the performance of this contract. Vendor shall describe, in an attachment if not already provided, the names and addresses of all authorized subcontractors to be utilized by Vendor in the performance of this contract, together with a description of the work to be performed by the subcontractor and the anticipated amount of money that each subcontractor is expected to receive pursuant to this contract. If required, Vendor shall provide a copy of any subcontracts within fifteen (15) days after execution of this contract. All subcontracts must include the same certifications that Vendor must make as a condition of this contract. Vendor shall include in each subcontract the subcontractor certifications as shown on the Standard Certification form available from the State. If at any time during the term of the Contract, Vendor adds or changes any subcontractors, then Vendor must promptly notify, by written amendment to the Contract, the State Purchasing Officer or the Chief Procurement Officer of the names and addresses and the expected amount of money that each new or replaced subcontractor will receive pursuant to the Contract. 30 ILCS 500/20-120.

4.4 AUDIT/RETENTION OF RECORDS: Vendor and its subcontractors shall maintain books and records relating to the performance of the contract or subcontract and necessary to support amounts charged to the State pursuant the contract or subcontract. Books and records, including information stored in databases or other computer systems, shall be maintained by the Vendor for a period of three (3) years from the later of the date of final payment under the contract or completion of the contract, and by the subcontractor for a period of three (3) years from the later of final payment under the term or completion of the subcontract. If Federal funds are used to pay contract costs, the Vendor and its subcontractors must retain their respective records for five (5) years. Books and records required to be maintained under this section shall be available for review or audit by representatives of: the procuring Agency, the Auditor General, the Executive Inspector General, the Chief Procurement Officer, State of Illinois internal auditors or other governmental entities with monitoring authority, upon reasonable notice and during normal business hours. Vendor and its subcontractors shall cooperate fully with any such audit and with any investigation conducted by any of these entities. Failure to maintain books and records required by this section shall establish a presumption in favor of the State for the recovery of any funds paid by the State under this contract or any subcontract for which adequate books and records are not available to support the purported disbursement. The Vendor or subcontractors shall not impose a charge for audit or examination of the Vendor's or subcontractor's books and records. 30 ILCS 500/20-65.

4.5 TIME IS OF THE ESSENCE: Time is of the essence with respect to Vendor's performance of this contract. Vendor shall continue to perform its obligations while any dispute concerning the contract is being resolved unless otherwise directed by the State.

4.6 NO WAIVER OF RIGHTS: Except as specifically waived in writing, failure by a Party to exercise or enforce a right does not waive that Party's right to exercise or enforce that or other rights in the future.

4.7 FORCE MAJEURE: Failure by either Party to perform its duties and obligations will be excused by unforeseeable circumstances beyond its reasonable control and not due to its negligence, including acts of nature, acts of terrorism, riots, labor disputes, fire, flood, explosion, and governmental prohibition. The non-declaring Party may cancel the contract without penalty if performance does not resume within thirty (30) days of the declaration.

4.8 CONFIDENTIAL INFORMATION: Each Party to this contract, including its agents and subcontractors, may have or gain access to confidential data or information owned or maintained by the other Party in the course of carrying out its responsibilities under this contract. Vendor shall presume all information received from the State or to which it gains access pursuant to this contract is confidential. Vendor information, unless clearly marked as confidential and exempt from disclosure under the Illinois Freedom of Information Act, shall be considered public. No confidential data collected, maintained, or used in the course of performance of the contract shall be disseminated except as authorized by law and with the written consent of the disclosing Party, either during the period of the contract or thereafter. The receiving Party must return any and all data collected, maintained, created or used in the course of the performance of the contract, in whatever form it is maintained, promptly at the end of the contract, or earlier at the request of the disclosing Party, or notify the disclosing Party in writing of its destruction. The foregoing obligations shall not apply to confidential data or information lawfully in the receiving Party's possession prior to its acquisition from the disclosing Party; received in good faith from a third Party not subject to any confidentiality obligation to the disclosing Party; now is or later becomes publicly known through no breach of confidentiality obligation by the receiving Party; or is independently developed by the receiving Party without the use or benefit of the disclosing Party's confidential information.

4.9 USE AND OWNERSHIP: All work performed or supplies created by Vendor under this contract, whether written documents or data, goods or deliverables of any kind, shall be deemed work for hire under copyright law and all intellectual property and other laws, and the State of Illinois is granted sole and exclusive ownership to all such work, unless otherwise agreed in writing. Vendor hereby assigns to the State all right, title, and interest in and to such work including any related intellectual property rights, and/or waives any and all claims that Vendor may have to such work including any so-called "moral rights" in connection with the work. Vendor acknowledges the State may use the work product for any purpose. For the avoidance of doubt, Vendor's System as described in Attachment I (Statement of Work), including updates, upgrades, and/or any modifications, is not work for hire, and is and shall remain Vendor's proprietary product to which subscription access is granted in accordance with Attachment I (Statement of Work) and Section 2.3 of this Agreement. Confidential data or information contained in such work shall be subject to confidentiality provisions of this contract.

4.10 INDEMNIFICATION AND LIABILITY: The Vendor shall indemnify and hold harmless the State of Illinois, its agencies, officers, employees, agents and volunteers from any and all costs, demands, expenses, losses, claims, damages, liabilities, settlements and judgments, including in-house and contracted attorneys' fees and expenses, arising out of: (a) any breach or violation by Vendor of any of its certifications, representations, warranties, covenants or agreements; (b) any actual or alleged death or injury to any person, damage to any real or personal property, or any other damage or loss claimed to result in whole or in part from Vendor's negligent performance; (c) any act, activity or omission of Vendor or any of its employees, representatives, subcontractors or agents; or (d) any actual or alleged claim that the services or goods provided under this contract infringe, misappropriate, or otherwise violate any intellectual property (patent, copyright, trade secret, or trademark) rights of a third party. In accordance with Article VIII, Section 1(a),(b) of the Constitution of the State of Illinois and 1973 Illinois Attorney General Opinion 78, the State may not indemnify private parties absent express statutory authority permitting the indemnification. Neither Party shall be liable for incidental, special, consequential, or punitive damages.

4.11 INSURANCE: Vendor shall, at all times during the term of this contract and any renewals or extensions, maintain and provide a Certificate of Insurance naming the State as an additionally insured for all required bonds and insurance. Certificates may not be modified or canceled until at least thirty (30) days' notice has been provided to the State. Vendor shall provide: (a) General Commercial Liability insurance in the amount of $1,000,000 per occurrence (Combined Single Limit Bodily Injury and Property Damage) and $2,000,000 Annual Aggregate; (b) Auto Liability, including Hired Auto and Non-owned Auto (Combined Single Limit Bodily Injury and Property Damage), in amount of $1,000,000 per occurrence; and (c) Worker's Compensation Insurance in the amount required by law. Insurance shall not limit Vendor's obligation to indemnify, defend, or settle any claims.

4.12 INDEPENDENT CONTRACTOR: Vendor shall act as an independent contractor and not an agent or employee of, or joint venture with the State. All payments by the State shall be made on that basis.

4.13 SOLICITATION AND EMPLOYMENT: Vendor shall not employ any person employed by the State during the term of this contract to perform any work under this contract. Vendor shall give notice immediately to the Agency's director if Vendor solicits or intends to solicit State employees to perform any work under this contract.

4.14 COMPLIANCE WITH THE LAW: The Vendor, its employees, agents, and subcontractors shall comply with all applicable federal, state, and local laws, rules, ordinances, regulations, orders, federal circulars and all license and permit requirements in the performance of this contract. Vendor shall be in compliance with applicable tax requirements and shall be current in payment of such taxes. Vendor shall obtain at its own expense, all licenses and permissions necessary for the performance of this contract.

4.15 BACKGROUND CHECK: Whenever the State deems it reasonably necessary for security reasons, the State may conduct, at its expense, criminal and driver history background checks of Vendor's and subcontractor's officers, employees or agents. Vendor or subcontractor shall immediately reassign any individual who, in the opinion of the State, does not pass the background check.

4.16 APPLICABLE LAW:

4.16.1 PREVAILING LAW: This contract shall be construed in accordance with and is subject to the laws and rules of the State of Illinois.

4.16.2 EQUAL OPPORTUNITY: The Department of Human Rights' Equal Opportunity requirements are incorporated by reference. 44 ILL. ADM. CODE 750.

4.16.3 COURT OF CLAIMS; ARBITRATION; SOVEREIGN IMMUNITY: Any claim against the State arising out of this contract must be filed exclusively with the Illinois Court of Claims. 705 ILCS 505/1. The State shall not enter into binding arbitration to resolve any dispute arising out of this contract. The State of Illinois does not waive sovereign immunity by entering into this contract.

4.16.4 OFFICIAL TEXT: The official text of the statutes cited herein is incorporated by reference. An unofficial version can be viewed at (*www.ilga.gov/legislation/ilcs/ilcs.asp*).

4.17 ANTI-TRUST ASSIGNMENT: If Vendor does not pursue any claim or cause of action it has arising under Federal or State antitrust laws relating to the subject matter of this contract, then upon request of the Illinois Attorney General, Vendor shall assign to the State all of Vendor's rights, title and interest in and to the claim or cause of action.

4.18 CONTRACTUAL AUTHORITY: The Agency that signs this contract on behalf of the State of Illinois shall be the only State entity responsible for performance and payment under this contract. When the Chief Procurement Officer or authorized designee or State Purchasing Officer signs in addition to an Agency, he/she does so as approving officer and shall have no liability to Vendor. When the Chief Procurement Officer or authorized designee or State Purchasing Officer signs a master contract on behalf of State agencies, only the Agency that places an order or orders with the Vendor shall have any liability to the Vendor for that order or orders.

4.19 EXPATRIATED ENTITIES: Except in limited circumstances, no business or member of a unitary business group, as defined in the Illinois Income Tax Act, shall submit a bid for or enter into a contract with a State agency if that business or any member of the unitary business group is an expatriated entity

4.20 NOTICES: Notices and other communications provided for herein shall be given in writing via electronic mail whenever possible. If transmission via electronic mail is not possible, then notices and other communications shall be given in writing via registered or certified mail with return receipt requested, via receipted hand delivery, via courier (UPS, Federal Express or other similar and reliable carrier), or via facsimile showing the date and time of successful receipt. Notices shall be sent to the individuals who signed this contract using the contact information following the signatures. Each such notice shall be deemed to have been provided at the time it is actually received. By giving notice, either Party may change its contact information.

4.21 MODIFICATIONS AND SURVIVAL: Amendments, modifications and waivers must be in writing and signed by authorized representatives of the Parties. Any provision of this contract officially declared void, unenforceable, or against public policy, shall be ignored and the remaining provisions shall be interpreted, as far as possible, to give effect to the Parties' intent. All provisions that by their nature

would be expected to survive, shall survive termination. In the event of a conflict between the State's and the Vendor's terms, conditions and attachments, the State's terms, conditions and attachments shall prevail.

4.22 PERFORMANCE RECORD / SUSPENSION: Upon request of the State, Vendor shall meet to discuss performance or provide contract performance updates to help ensure proper performance of the contract. The State may consider Vendor's performance under this contract and compliance with law and rule to determine whether to continue the contract, suspend Vendor from doing future business with the State for a specified period of time, or whether Vendor can be considered responsible on specific future contract opportunities.

4.23 FREEDOM OF INFORMATION ACT: This contract and all related public records maintained by, provided to or required to be provided to the State are subject to the Illinois Freedom of Information Act (FOIA) (50 ILCS 140) notwithstanding any provision to the contrary that may be found in this contract.

4.24 SCHEDULE OF WORK: Any work performed on State premises shall be done during the hours designated by the State and performed in a manner that does not interfere with the State and its personnel.

4.25 WARRANTIES FOR SUPPLIES AND SERVICES:

4.25.1. Vendor warrants that the System will (a) comply with the requirements established under this Contract, all federal and state laws, regulations and ordinances applicable to the System; and (b) not infringe any United States patent, copyright or other intellectual property rights of any third party. Vendor agrees to reimburse the State for any losses, costs, damages or expenses, including without limitations, reasonable attorney's fees and expenses, arising from failure of the System to meet such warranties.

4.25.2. Vendor warrants that all services will be performed to meet the requirements of this contract in an efficient and effective manner by trained and competent personnel. Vendor shall monitor performances of each individual and shall immediately reassign any individual who does not perform in accordance with this contract, who is disruptive or not respectful of others in the workplace, or who in any way violates the contract or State policies.

4.26 REPORTING, STATUS AND MONITORING SPECIFICATIONS: Vendor shall immediately notify the State of any event that may have a material impact on Vendor's ability to perform this contract.

EMPLOYMENT TAX CREDIT: Vendors who hire qualified veterans and certain ex-offenders may be eligible for tax credits. 35 ILCS 5/216, 5/217. Please contact the Illinois Department of Revenue (telephone #: 217-524-4772) for information about tax credits.

5. SUPPLEMENTAL PROVISIONS

In the event of a conflict between the State's and the Vendor's terms, conditions, and attachments, the State's terms, conditions and attachments shall prevail.

5.1. STATE SUPPLEMENTAL PROVISIONS

☒ Attachment B-1, IDES Supplemental Terms and Conditions

☒ Attachment B-2, Federal Funding Certifications and Assurances

☒ Attachment B-3, Protection of Social Security Numbers: Contractor/Subcontractor Policy Statement

☒ Attachment B-4, Security Requirements for Cloud-Based Technology

5.2. VENDOR SUPPLEMENTAL PROVISIONS

☒ Attachment I, Statement of Work

☒ Attachment II, Overview of Pondera Fraud Detection & Case Management

ATTACHMENT B-1

IDES SUPPLEMENTAL TERMS AND CONDITIONS

1. Confidential Information – Section 1900; Part 603:

The Parties agree that if a conflict arises under the performance of this contract in construing the terms of this Section 1 of IDES Supplemental Terms And Conditions, *Confidential Information – Section 1900; Part 603*, and any other provision of this Contract, the terms of this Section 1 shall control.

(a) In Vendor's performance of this contract, it and its employees and agents will have access to documents, files, records or other information that are confidential within the meaning of Section 1900 of the Unemployment Insurance Act, 820 ILCS 405/1900 ("Section 1900"), and federal regulations codified at 20 CFR Part 603, and in particular 20 CFR 603.9 ("Part 603"). VENDOR hereby assures and confirms that it and its employees and agents are subject to and shall comply with all provisions of Section 1900 and Part 603, including without limitation provisions pertaining to the protection from unauthorized use and/or disclosure of said confidential information and penalties for noncompliance. Protection from unauthorized use and/or disclosure specifically includes storage in a place physically secure from access by unauthorized persons, maintaining information in electronic formats such as magnetic tapes, discs, or on servers in such a way that unauthorized persons cannot obtain the information by any means, and undertaking precautions to ensure that only authorized employees and agents have access to said confidential information. Any dissemination or use of said confidential information other than for the purpose of this contract without the express written authority of the Director of IDES is specifically prohibited.

(b) Vendor hereby certifies that all employees and agents who are given access to said confidential information under this contract shall be instructed about the confidentiality requirements contained in this Section 1 and that said employees and agents shall adhere to same, and agrees to report any infraction by any employee or agent to IDES fully and promptly. Vendor shall restrict access to said confidential information to only those employees and agents who require access in the performance of this contract. Vendor shall not subcontract this contract or any portion of this contract without the prior written approval of IDES, and any such subcontractor and said subcontractor's employees and agents shall be expressly subject to the provisions of this Section 1. Notwithstanding any other provision of the contract to the contrary, this contract is subject to immediate cancellation by IDES for failure of Vendor or Vendor's subcontractors or any of their employees or agents to adhere to the provisions of this Section 1.

2. Unemployment Insurance Contributions / Unemployment Insurance Employer Account Number:

Vendor certifies that:

(a) Vendor is not delinquent in the payment of contributions, payments in lieu of contributions, penalties and/or interest as required of it under the Illinois Unemployment Insurance (UI) Act, nor does it owe any sums to the State because of overpaid UI benefits;

(b) Vendor's current and correct Illinois UI employer account number (if applicable) is: _____; and

(c) Vendor has disclosed its current and correct Federal Employer Identification Number (FEIN) in the space provided on the Taxpayer Identification Number form included in this contract, which is the same FEIN the Vendor has disclosed to the State for UI purposes.

Vendor acknowledges and agrees that if for any reason the Vendor's FEIN changes, the Vendor shall immediately notify the State of the new FEIN in writing, transmitted by telefax to the IDES Office of Legal Counsel at 312-793-2164, with such notice to include reference to the applicable IDES or CMS contract number assigned to this contract. Upon receipt of such notice, all further payments under this CONTRACT shall be processed under the new FEIN.

Vendor further acknowledges and agrees that the State has the right to withhold from any sum or sums otherwise payable to the Vendor pursuant to this contract the amount(s) of any past due contributions, payments in lieu of contributions, penalties, interest, and/or overpaid benefits it may owe under the UI Act, and to apply such amount(s) so withheld toward satisfaction of any such past due contributions, payments in lieu of contributions, penalties, interest, and/or overpaid benefits, and hereby expressly authorizes the State to do so.

Signature: [redacted] Date: 09/10/20

IDES ATTACHMENTS

ATTACHMENT B-2
(10/2015)

FEDERAL FUNDING CONTRACT REQUIREMENTS AND CERTIFICATIONS

The U.S. Office of Management and Budget (OMB) and the U.S. Department of Labor (DOL) require the following certifications and contract requirements to be included in contracts and subcontracts funded in whole or part with Federal financial assistance. Since Vendor's contract is so funded, Vendor certifies and assures as follows and agrees to include the following certifications and assurances in each subcontract with any subcontractors Vendor may hire to perform all or part of the work covered by the contract:

1. Federal Cost Principals and Audit Requirements:

The federal cost principles and audit requirements of this contract are governed by the cost principles and audit requirements of OMB found in 2 CFR Part 200, as amended (Part 200), and of DOL found in 2 CFR Part 2900, as amended (Part 2900), the successor regulations to OMB Circulars No. A-87 and No. A-133, 2 CFR Part 225 (OMB), and 29 CFR Parts 96 and 99 (DOL). Vendor acknowledges that for purposes of this contract and Parts 200 and 2900, Vendor is a Contractor as defined under 2 CFR 200.23 and not an Auditee, Non-Federal entity, Recipient, nor Subrecipient as defined under 2 CFR 200.6, 200.69, 200.86, and 200.93 respectively.

2. Mandatory State Energy Efficiency Standards and Policies (As Applicable):

As applicable, the mandatory standards and policies, if any, relating to energy efficiency that are contained in the State energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6201) are incorporated herein in their entirety.

3. Contracts > $10,000 (If Not Provided Elsewhere) / Termination For Cause & Remedies; Termination For Convenience:

If not provided for elsewhere in this contract, and if the value of this contract is more than $10,000, the following provisions are part of this contract:

(a) Termination for Cause and Remedies.

The State may terminate this contract, in whole or in part, immediately upon notice to the Vendor if: (a) the State determines that the actions or inactions of the Vendor, its agents, employees or subcontractors have caused, or reasonably could cause, jeopardy to health, safety, or property, or (b) the Vendor has notified the State that it is unable or unwilling to perform the contract.

If Vendor fails to perform to the State's satisfaction any material requirement of this contract, is in violation of a material provision of this contract, or the State determines that the Vendor lacks the financial resources to perform the contract, the State shall provide written notice to the Vendor to cure the problem identified within the period of time specified in the State's written notice. If not cured by that date the State may either: (a) immediately terminate the contract without additional written notice, or (b) enforce the terms and conditions of the contract.

For termination due to any of the causes contained herein, the State retains its rights to seek any available legal or equitable remedies and damages.

(b) Termination for Convenience.

The State may, for its convenience and with 30 days prior written notice to Vendor, terminate this contract in whole or in part and without payment of any penalty or incurring any further obligation to the Vendor. The Vendor shall be entitled to compensation upon submission of invoices and proof of claim for supplies and services provided in compliance with this contract up to and including the date of termination.

4. Contracts ≥ $100,000 or More / Anti-Lobbying Certification:

If the value of this contract is $100,000 or more, Vendor certifies that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Vendor also certifies that it has disclosed to the State any lobbying with non-Federal funds that took or takes place in connection with obtaining any such Federal award.

5. Contracts > $150,000 / Clean Air Act & Federal Water Pollution Control Act Certification:

If the value of this contract is more than $150,000, Vendor certifies that it shall comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251–1387).

6. Suspension, Debarment, Exclusion, or Disqualification from Contract Certification:

Vendor certifies that it and its principals are not prohibited from participating in this contract because it or any of its principals are suspended, debarred, proposed for debarment, excluded (voluntarily or otherwise), or disqualified under 29 CFR Part 98, and that it will comply with 29 CFR Part 98 as a condition of participating in this contract and will require, if applicable, any subcontractor(s) to comply with 29 CFR Part 98 as a condition of participating in any subcontract(s) under this contract. This certification includes, without limitation, Vendor's certification that it is not listed on the government-wide Excluded Parties List System in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1986 Comp., p. 189) and 12689 (3 CFR Part 1989 Comp., p. 235), "Debarment and Suspension."

7. Nondiscrimination and Equal Opportunity under the Workforce Innovation and Opportunity Act Certification:

Vendor certifies that it will comply fully with the nondiscrimination and equal opportunity regulations implemented under Title I of the Workforce Innovation and Opportunity Act of 2014, as amended (WIOA), which are codified at 29 CFR Part 37 and incorporated herein by reference, and which require full compliance with: Section 188 of WIOA; Title VI of the Civil Rights Act of 1964, as amended; Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975, as amended; title IX of the Education Amendments of 1972, as amended; and 29 CFR Part 37 and all other regulations implementing the laws listed above. The United States has the right to seek judicial enforcement of this assurance.

IDES ATTACHMENTS

ATTACHMENT B-3

PROTECTION OF SOCIAL SECURITY NUMBERS
CONTRACTOR/SUBCONTRACTOR POLICY STATEMENT

The Identity Protection Act, 5 ILCS 179/1 *et seq*. ("IPA"), requires the Illinois Department of Employment Security ("IDES") to implement certain policies and procedures to protect Social Security numbers ("SSN" or "SSNs") used in the administration of IDES programs and services, including SSNs disclosed to other entities when disclosure is necessary to the performance of IDES duties and responsibilities. Under the IPA, before SSNs may be disclosed to contractors or subcontractors IDES must obtain in writing the policies the contractors or subcontractors will follow to protect the disclosed SSNs in accord with the requirements of the IPA.

This policy statement will serve as written acknowledgement by the undersigned contractor or subcontractor ("Recipient") that any and all SSNs disclosed by IDES will be protected in accord with the policies set forth herein:

1. The Recipient acknowledges that any SSNs disclosed by IDES will be utilized solely for the specific purpose(s) and use(s) identified in the pertaining contract, subcontract, grant, subgrant, or other agreement between IDES and the Recipient ("Agreement"). The Recipient affirms that it will not utilize any disclosed SSNs other than for said purpose(s) and use(s) without the prior written consent of IDES, and that it will not archive or retain any disclosed SSNs in any manner, form, or format after the termination of the Agreement.

2. The Recipient affirms that only the officers and employees of the Recipient who have a need to access disclosed SSNs for the purpose(s) and use(s) identified in the Agreement will have access to disclosed SSNs. The Recipient also affirms that it is responsible for enforcing this restriction of access to disclosed SSNs, and that all of the officers and employees of the Recipient who will have access to disclosed SSNs have been trained to protect the confidentiality of SSNs in accord with this policy statement. Training shall include instructions on proper handling of disclosed SSNs from receipt through disposal (see Paragraph 7).

3. The Recipient acknowledges that all SSNs disclosed by IDES are confidential and will be protected from unauthorized use and/or disclosure. Protection from unauthorized use and/or disclosure includes:
   a) Restricting access to disclosed SSNs to authorized personnel in accord with Paragraph 2;
   b) Storing materials, documents, or media containing disclosed SSNs in a place and/or manner physically secure from access by unauthorized persons;
   c) Maintaining disclosed SSNs reduced to electronic or digital media or formats such as magnetic tapes, hard drives, flash drives, CDs or server-based applications in such a way that unauthorized persons cannot access or obtain disclosed SSNs by any means; and
   d) Applying security measures to computer systems ensuring that only authorized personnel will have access to disclosed SSNs accessible through said computer systems.

4. The Recipient affirms that it complies with all applicable laws, regulations, and State and federal legal authorities relating to the protection of disclosed SSNs, including, without limitation:
   a) Federal regulations codified at 20 CFR 603 pertaining to recipients of unemployment compensation information;
   b) The Illinois Data Processing Confidentiality Act, 30 ILCS 585/0.01 *et seq.*;
   c) Section 1900 of the Illinois Unemployment Insurance Act, 820 ILCS 405/1900; and
   d) Section 10(c)(1) of the IPA, 5 ILCS 179/10(c)(1).

5. The Recipient affirms that it will not subcontract, subgrant, or otherwise transfer or assign any of the Recipient's duties or obligations involving disclosed SSNs under the Agreement without the prior written consent of IDES, and/or the approval and/or execution of an appropriate subcontract, subgrant, or other third-party agreement by IDES.

6. The Recipient affirms that it will retain records of access to and use of disclosed SSNs for a period of three years following receipt of the SSNs, and will allow on-site inspections by IDES to verify SSN security and usage as well as audit access during the three year period after the receipt of the SSNs. The Recipient also affirms that it will correct any security and/or usage deficiency(ies) identified by IDES promptly upon receipt of written notice of said deficiency(ies).

7. The Recipient acknowledges that the materials, documents, or media of any type or form that contain SSNs disclosed by IDES are the property of and shall be returned to IDES upon request. The Recipient also acknowledges that it is responsible for the disposal of said materials, documents, or media upon termination of the Agreement. "Disposal"" means the return or delivery of said materials, documents, or media to IDES, or the destruction of same, as directed by IDES.

Pondera Solutions, LLC
Recipient

Name: [redacted]
(Print)

By: [redacted]
(Signature)

Title: Sr. Vice President

Date: 09/10/20

ATTACHMENT B-4
SECURITY REQUIREMENTS FOR CLOUD-BASED TECHNOLOGY

The Vendor agrees and acknowledges that it shall comply with the following security requirements:

- Vendor will notify the State's Chief Information Security Officer within 24 hours of any information breach or other security incident which impacts the State's data.

- Vendor shall have a documented security incident policy and plan. Vendor must supply a copy at the request of the State of Illinois.

- Vendor must comply with all Federal and State laws, rules and regulations. *(See Appendix S1)*

- Vendor must comply with all State of Illinois Enterprise Security Policies (https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx).

- Vendor's system must meet State of Illinois accessibility requirement as defined in the *Illinois Information Technology Accessibility Act*. If available, Vendor must provide the State of Illinois their most recent Voluntary Product Accessibility Template (VPAT).

- Vendor program and project management personnel must ensure coordination of activities with State of Illinois Governance program. Vendor must comply will all policies, standards and procedures defined by the State of Illinois' Department of Innovation and Technology's Enterprise Portfolio Management Office.

- Vendor's system must have the ability to interface with the State's Identity and Access Management solutions if credentialing is required.

- Vendor's system must have the ability to log activity within the system and have the ability to forward log information to the State's security incident and event management system (SIEM). Vendor must meet the State of Illinois' Minimum Logging Requirements. *(See Security Appendix S2)*

  Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State with System Operation Controls report (SOC 2) annually and applicable or Bridge/Gap letter.

- Vendor must perform an annual risk assessment and data classification and system categorization process. This formal risk assessment will be provided to the State of Illinois.

- If the vendor cannot provide a SOC report and Bridge/Gap letter, or 3rd party risk assessment the Vendor must perform an internal security controls assessment to demonstrate compliance with

the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system. The vendor must provide attestation of compliance along with the results of this assessment documented in a Security Assessment Report (SAR) to the State of Illinois.
(See Security Appendix S3)

- Vendor must provide a Plan of Action and Milestones (POA&M) to the State of Illinois that addresses any control deficiencies identified during an external third party SOC 2 audit or an internal security controls assessment based on the current revision of NIST 800-53 for a moderate system.
(see Security Appendix S4)

- Vendor must complete and provide the State of Illinoisa System Security Plan (SSP) that is consistent with NIST 800-18. This SSP must be reviewed annually.
(See Security Appendix S5)

- Vendor must ensure all hosted data pertinent to this contract remains located within the contiguous United States.

- Vendor must ensure encryption of State of Illinois data at rest and in motion. This encryption must comply with encryption security controls as defined in the most current version of FIPS 140 using AES encryption with a minimum key length of 256 bits. Vendor must provide proof of encryption.

- Vendor must be store data in a non-proprietary format or vendor must provide a solution to extract any State of Illinois data stored in the vendor's solution.

- Vendor must only use State or Participant data, State-related or Participant-related data, and/or approved third party data for the purposes stated in this contract.

- Vendor must maintain a robust and reliable data backup system. Vendor must supply a description of backup methodology and this methodology must meet defined MTD and RPO requirements.

- Vendor must provide a disaster recovery mythology and provide proof of annual disaster recovery testing, including issues discovered and remediation plans for the issues discovered.

- Vendor must ensure that production data is used only throughout the production environment deployment process.

- Vendor must provide a copy of all data to the State without delay upon request by the State.

- Upon contract termination, Vendor must provide a copy of all data to the State and sanitize all media that contained State of Illinois data. For sanitization, Vendor must use the current revision of NIST Special Publication 800-88 "Guidelines for Media Sanitization". Vendor must provide certification of media sanitization including the method, date and time.

- Vendor and/or its agents must not resell nor otherwise redistribute information gained from its access to the State or Participants.

- Vendor must not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the State.

- Vendor must remediate critical, high and medium vulnerabilities within the application that are detected during the security assessments and are determined by the State of Illinois to pose an unacceptable risk.

- Vendor must secure independent 3rd party penetration testing at regular intervals according to Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) recommendations. Vendor must provide an executive summary report and any corrective action plan to the State of Illinois upon request.

Agreed to and accepted by Vendor:

By: [redacted]

Printed: [redacted]

Title: Sr. Vice President

Date: 09/10/20

Security Appendix S1 – Federal and State laws, rules and regulations –

- Federal regulations codified at 20 CFR 603 pertaining to recipients of unemployment compensation information
- The Illinois Data Processing Confidentiality Act, 30 ILCS 585/0.01 et seq.
- Section 1900 of the Illinois Unemployment Insurance Act, 820 ILCS 405/1900
- Illinois Identity Protection Act (5 ILCS 179)
- Illinois Personal Information Protection Act (815 ILCS 530)
- Social Security Administration

Security Appendix S2 – Minimum Logging Requirements

- Input validation failures e.g. protocol violations, unacceptable encodings, invalid parameter names and values
- Output validation failures e.g. database record set mismatch, invalid data encoding
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures e.g. cookie session identification value modification
- Application errors and system events e.g. syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes
- Application and related systems start-ups and shut downs, and logging initialization (starting, stopping or pausing)
- Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads

Security Appendix S3: Security Controls for Vendors

Authoritative Document NIST 800-53 v4 – Security and Privacy Controls

Access and Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AC Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Access Control Policy and Procedures	AC-1	
• Account Management	AC-2	(1), (2), (3), (4)
• Access Enforcement	AC-3	
• Information Flow Enforcement	AC-4	
• Separation of Duties	AC-5	
• Least Privilege	AC-6	(1), (2), (5), (9), (10)
• Unsuccessful Logon Attempts	AC-7	
• System Use Notification	AC-8	
• Session Lock	AC-11	(1)
• Session Termination	AC-12	
• Permitted Actions without Identification or Authentication	AC-14	
• Remote Access	AC-17	(1), (2), (3), (4)
• Wireless Access	AC-18	(1)
• Access Control for Mobile Devices	AC-19	(5)
• Use of External Information Systems	AC-20	(1), (2)
• Information Sharing	AC-21	
• Publicly Accessible Content	AC-22	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Awareness and Training (AT)

Organizations must (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

AT - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Security Awareness and Training Policy and Procedures	AT-1	
• Security Awareness Training	AT-2	(2)
• Role-Based Security Training	AT-3	
• Security Training Records	AT-4	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

AU - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Audit and Accountability Policy and Procedure	AU-1	
• Audit Events	AU-2	(3)
• Content of Audit Records	AU-3	(1)
• Audit Storage Capacity	AU-4	
• Response to Audit Processing Failures	AU-5	
• Audit Review, Analysis, and Reporting	AU-6	(1), (3)
• Audit Reduction and Report Generation	AU-7	(1)
• Time Stamps	AU-8	(1)
• Protection of Audit Information	AU-9	(4)
• Audit Record Retention	AU-11	
• Audit Generation	AU-12	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Security Assessment and Authorization Policy and Procedures	CA-1	
• Security Assessments	CA-2	(1)
• System Interconnections	CA-3	(5)
• Plan of Action and Milestones	CA-5	
• Security Authorization	CA-6	
• Continuous Monitoring	CA-7	(1)
• Internal System Connections	CA-9	

Authority	
NIST	SP 800-53 Security and Privacy Controls
NIST	SP 800-53A Assessing Security Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

CM - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Configuration Management Policy and Procedures	CM-1	
• Baseline Configuration	CM-2	(1), (3), (7)
• Configuration Change Control	CM-3	(2)
• Security Impact Analysis	CM-4	
• Access Restrictions for Change	CM-5	
• Configuration Settings	CM-6	
• Least Functionality	CM-7	(1), (2), (4)
• Information System Component Inventory	CM-8	(1), (3), (5)
• Configuration Management Plan	CM-9	
• Software Usage Restrictions	CM-10	
• User-Installed Software	CM-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Contingency Planning Policy and Procedures	CP-1	
• Contingency Plan	CP-2	(1), (3), (8)
• Contingency Training	CP-3	
• Contingency Plan Testing	CP-4	(1)
• Alternate Storage Site	CP-6	(1), (3)
• Alternate Processing Site	CP-7	(1), (2), (3)
• Telecommunications Services	CP-8	(1), (2)
• Information System Backup	CP-9	(1)
• Information System Recovery and Reconstitution	CP-10	(2)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.

IA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Identification and Authentication Policy and Procedures	IA-1	
• Identification and Authentication (Organizational Users)	IA-2	(1), (2), (3), (8), (11), (12)
• Device Identification and Authentication	IA-3	
• Identifier Management	IA-4	
• Authentication Management	IA-5	(1), (2), (3), (11)
• Authenticator Feedback	IA-6	
• Cryptographic Module Authentication	IA-7	
• Identification and Authentication (Non-Organizational Users)	IA-8	(1), (2), (3), (4)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and or authorities.

IR - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Incident Response Policy and Procedures	IR-1	
• Incident Response Training	IR-2	
• Incident Response Testing	IR-3	(2)
• Incident Handling	IR-4	(1)
• Incident Monitoring	IR-5	
• Incident Reporting	IR-6	(1)
• Incident Response Assistance	IR-7	(1)
• Incident Response Plan	IR-8	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

MA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System Maintenance Policy and Procedures	MA-1	
• Controlled Maintenance	MA-2	
• Maintenance Tools	MA-3	(1), (2)
• Nonlocal Maintenance	MA-4	(2)
• Maintenance Personnel	MA-5	
• Timely Maintenance	MA-6	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

MP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Media Protection Policy and Procedures	MP-1	
• Media Access	MP-2	
• Media Marking	MP-3	
• Media Storage	MP-4	
• Media Transport	MP-5	(4)
• Media Sanitization	MP-6	
• Media Use	MP-7	(1)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PE - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Physical and Environmental Protection Policy and Procedures	PE-1	
• Physical Access Authorizations	PE-2	
• Physical Access Control	PE-3	
• Access Control for Transmission Medium	PE-4	
• Access Control for Output Devices	PE-5	
• Monitoring Physical Access	PE-6	(1)
• Visitor Access Records	PE-8	
• Power Equipment and Cabling	PE-9	
• Emergency Shutoff	PE-10	
• Emergency Power	PE-11	
• Emergency Lighting	PE-12	
• Fire Protection	PE-13	(3)
• Temperature and Humidity Controls	PE-14	
• Water Damage Protection	PE-15	
• Delivery and Removal	PE-16	
• Alternate Work Site	PE-17	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individual's accessing the information systems.

PL - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Security Planning Policy and Procedures	PL-1	
• System Security Plan	PL-2	(3)
• Rules of Behavior	PL-4	(1)
• Information Security Architecture	PL-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information system are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

PS - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Personnel Security Policy and Procedures	PS-1	
• Position Risk Designation	PS-2	
• Personnel Screening	PS-3	
• Personnel Termination	PS-4	
• Personnel Transfer	PS-5	
• Access Agreements	PS-6	
• Third-Party Personnel Security	PS-7	
• Personnel Sanctions	PS-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

RA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Risk Assessment Policy and Procedures	RA-1	
• Security Categorization	RA-2	
• Risk Assessment	RA-3	
• Vulnerability Scanning	RA-5	(1), (2), (5)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizations information system; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and or services outsourced from the organization.

SA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Services Acquisition Policy and Procedures	SA-1	
• Allocation of Resources	SA-2	
• System Development Life Cycle	SA-3	
• Acquisition Process	SA-4	(1), (2), (9), (10)
• Information System Documentation	SA-5	
• Security Engineering Principles	SA-8	
• External Information System Services	SA-9	(2)
• Developer Configuration Management	SA-10	
• Developer Security Testing and Evaluation	SA-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e. information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries for the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organization information systems.

SC - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Communication Protection Policy and Procedures	SC-1	
• Application Partitioning	SC-2	
• Information in Shared Resources	SC-4	
• Denial of Service Protection	SC-5	
• Boundary Protection	SC-7	(3), (4), (5), (7)
• Transmission Confidentiality and Integrity	SC-8	(1)
• Network Disconnect	SC-10	
• Cryptographic Key Establishment and Management	SC-12	
• Cryptographic Protection	SC-13	
• Collaborative Computing Devices	SC-15	
• Public Key Infrastructure Certificates	SC-17	
• Mobile Code	SC-18	
• Voice Over Internet Protocol	SC-19	
• Secure Name/Address Resolution Service (Authoritative Source)	SC-20	
• Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	
• Architecture and Provisioning for Name/Address Resolution Service	SC-22	
• Session Authenticity	SC-23	
• Protection of Information at Rest	SC-28	
• Process Isolation	SC-39	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information systems flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems, and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

SI - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Information Integrity Policy and Procedures	SI-1	
• Flaw Remediation	SI-2	(2)
• Malicious Code Protection	SI-3	(1), (2)
• Information System Monitoring	SI-4	(2), (4), (5)
• Security Alerts, Advisories and Directives	SI-5	
• Software, Firmware, and Information Integrity	SI-7	(1), (7)
• Spam Protection	SI-8	(1), (2)
• Information Input Validation	SI-10	
• Error Handling	SI-11	
• Information Handling and Retention	SI-12	
• Memory Protection	SI-16	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Security Appendix S4 - Plan of Actions and Milestones Template

Identified Deficiency	Residual Risk	Detailed Remediation Plan

ATTACHMENT I

STATEMENT OF WORK (SOW)

Pondera Solutions LLC (Pondera or Vendor) will deliver to the Illinois Department of Employment Security (IDES) its fraud analytics (FraudCaster®) and case management (CaseTracker™) solutions (FraudCaster and CaseTracker, collectively, the System) together with related implementation services, all as more particularly described in this SOW. This SOW is attached to the Contract (No. 4100132391) between IDES and Pondera (the "Contract"). In the event of conflict between the Contract and this SOW, the terms and conditions of the Contract shall prevail.

1. SCOPE OF SERVICES

A. Pondera will deliver FraudCaster as a Software-as-a-Service subscription deployed in Microsoft's Azure environment for unlimited users. The specific FraudCaster functionality and any applicable quantities or limitations to be delivered is as follows:

Activity	Description	Quantity
Claimant Validation	Pondera will run current claimants through FraudCaster to identify areas of risk such as shared values (such as home address, IP address, e-mail address), deceased participants, behavioral pattern matching, and other anomalies. Results trigger alerts and populate the claimant profiles.	Up to 1,100,000 profile
Employer Validation	Pondera will run existing employers through FraudCaster to identify areas of risk. Results trigger alerts and populate the employer profiles.	Up to 375,000 profiles
Procedural Flagging	Pondera will configure and deploy alerts to check anomalies. Results will trigger alerts on the Dashboard and will be added to claimant and employer Profiles.	Up to 20 flags
Geospatial Analysis	Pondera will geocode claimant and employer data for use in geospatial analysis to analyze relationships across participants.	Up to 3 maps
Street View	FraudCaster will provide street-level mapping to view claimant and employer locations from within the dashboard.	Up to 1,500,000 Entities
Data Matching	FraudCaster matches IDES enrollment data for claimants and employers against multiple lists such as the SSA DMF and more.	Up to 1,500,000
Scorecard	The FraudCaster Claimant Scorecard provides users with ready access to claimants and their associated risk score.	1 Claimant Scorecard
Fictitious Employer Schemes	FE Schemes allows users to view and compare behaviors of businesses and their claimants with aggregated patterns over time	1 FE Dashboard
Network Analyzer	Pondera will provide our link analysis module for case investigation.	Up to 5 templates

In addition to the above-described FraudCaster functionality, Pondera will include the stated quantities of the following 3 key Thomson Reuters CLEAR components:

- 10 CLEAR Investigations Advanced passwords with real-time access to data from credit bureaus, vehicles, reverse phone, social media, utilities, and more. Includes additional access to criminal records, real property, liens/bankruptcies, family members, and associates.
- CLEAR ID Confirm Batch Reports for up to 1,250 claimants per day for verifying identity of new claimants.

- One-time CLEAR ID Confirm Batch Reports for initial claimants from 3/1/2020 to 9/15/2020 to verify the identity of current claimants (estimated to be 1,100,000 unique claimants)

B. Pondera will deliver the following CaseTracker components for up to 10 users in the quantities set forth:

Activity	Description	Quantity
Intake Form	The intake form is used to record new cases.	1
Workflow	Workflow rules are used to optimize the business process. A 'rule' is logic that triggers a change in status.	Up to 7
Case Record	The case record will contain all the standard case functionality including those items in Case Details section.	No limit
Case Details Overview	This tab displays information on the intake form and includes up to 150 fields (closure reason, recommended outcome, etc.).	No limit
Case Activity	Record Notes Record To□Do's with reminders Assign To□Do's to a CaseTracker user other than case owner Send and receive emails from within a case.	No limit
Case Entities	Add multiple entities to a case to record various 'Entity Types' (i.e. customer, subject, witness, etc.). Each of the unique forms may have up to 50 data fields.	Up to 3
Case Files	Attach any sort of electronic document to the case (fax, scanned document, MS Word, etc.) with a maximum individual attachment size of 200 MB.	No limit
General Case Features	Ability to assign a case by selecting an owner from the pick list and the ability to print the case file. There is also case history that will display an audit trail of changes made to the case record.	No limit
Integration with Current System	Pondera can import cases from the existing case management system. Many clients choose to import active cases only.	No limit
Case Record Forms	Forms can be deployed within the case file to record information. Forms are used for data sets that must be recorded more than once during the case lifecycle. For example: An expense form could be deployed to track many expense items. An interview form could be deployed to record every interview conducted.	Up to 7
Maintenance	Pondera provides the following maintenance functions: ▪ Add, modify or delete users, select their access level and notify them by email of their username and password ▪ Add, modify or delete category items (issues, products, etc.) ▪ Add, modify or delete workflow rules (for example: users may change timing of notifications) ▪ Add, modify or delete email standard responses	No limit
Access Controls	Access controls restrict functions and data available to groups of users. For example, information may be restricted based on the user's department. In that case, the user only sees cases and report information related to that department. Other examples could include case type, location, severity, etc.	Up to 5 roles
Reporting	CaseTracker includes a standard reporting package. This is an ad-hoc reporting tool integrated in case management and will be populated with reportable field values. Pondera will provide reports based on the IDES requirements, such as audit or investigation outcomes, progress of prosecution referrals and hearings, and performance, to monitor program integrity efforts.	Up to 7 pre-configured reports and 4 ad-hoc reporting licenses

Activity	Description	Quantity
Automated steps	Built in processes to allow users to configure specific functions including transferring a complaint to a case, case assignment, set notifications for updates related to records submissions, reporting dates, field population, dependencies, form indicators etc.	Up to 8 business rules
Search options on Advanced Search and Case View	Ability to search within CaseTracker to identify potentially related cases or providers.	Up to 5 search criteria
Time & Expense Tracking	CaseTracker includes a standard employee time and case expense tracking functionality. This facilitates the seamless creation of employee routine timesheets and investigative costs.	No limit

C. Pondera will provide the following training for the System:

1) Prior to go-live, Pondera will conduct on-site training sessions (absent any in-person restrictions due to COVID-19) for each IDES stakeholder group identified during the kickoff meeting. We will provide this training on the actual system and it includes customized, screen-specific user manuals. Pondera will use a combination of the following training:

- Onsite classroom training prior to go-live
- Web-based User Manual embedded directly in Pondera's dashboard tab
- One-on-One Training (remote, on-demand)

2) Pondera will also provide scheduled 30- to 60-minute intervals of personalized training, on an as-needed basis, for any user in need of additional training or support. These can be scheduled by request to cover or review a specialized skill set or to train new hires.

3) Throughout the term of this SOW, Pondera will conduct refresh-training courses for the Pondera System, both on-site and via web conferencing. These training sessions provide guidance for all users as well as specific break-outs based on system roles. In addition, Pondera is available for scheduled web-based training sessions, as requested. Pondera will provide annual onsite follow-up training after the initial implementation for analytics, case tracking, and reporting.

4) Pondera will provide an online User Manual for the Pondera System as described in Section 2 of this SOW. There is also user help within the application in the forms of contextual help and FAQs.

D. Pondera will provide the following Help Desk support for the Pondera System:

Throughout the term of this SOW, Pondera will provide both product and Help Desk support. Live phone support is available Monday through Friday from 08:00 CT to 17:00 CT, excluding Federal holidays. Access to the Pondera electronic ticketing system is available 24 hours a day, 7 days a week, and 365 days a year except for scheduled maintenance windows.

All authorized users can submit support requests via email, phone, or by directly logging them into the customer support portal. Pondera will respond to all support tickets submitted through the customer support portal during non-business hours in the next business day. Submitting a support request via email automatically creates a support ticket and an acknowledgement email, when a support ticket number is sent. Once a ticket is created, additional stakeholders / managers can monitor the status of support tickets at any time. Each support request must include:

- A description of the support ticket and an assessment of its severity
- A description of the events leading up to the need to create a support ticket (if applicable)
- Screenshots of the dashboard or system screen related to the problem (if applicable)

Every support ticket receives a tracking number and is assigned to a support professional depending on its severity level. Pondera identifies three support ticket severity levels, based on urgency and impact. The following table indicates the severity levels for support tickets, a description of what defines the severity of a support ticket, and the response time for each severity level:

Issue Severity Level	Severity Level Description	Issue Response Time
High	An issue that impacts all IDES users of the Pondera System. The entire or partial use of the Pondera production system is impacted such that there is complete loss of service or system functionality for which there is no workaround. The operation is mission critical to the business and the situation is an emergency.	Four (4) hours
Medium	An issue that impacts multiple IDES users or a portion of the Pondera System. Use of the Pondera production system is impacted such that important features or functions do not operate properly but acceptable temporary workarounds exist. Normal operation can continue with workarounds.	One (1) business day
Low	An issue that impacts neither the Pondera System nor IDES's use or access to the Pondera System such that the impact is an inconvenience or a minor deficiency. The overall performance and/or system integrity is unaffected.	Two (2) business days

Pondera will assign a member of the Special Investigations (SIU) to work with IDES investigations and enforcement staff. IDES may include Pondera's assigned SIU member in their regular activities such as SIU team meetings and enforcement debriefs.

The assigned SIU member will assist IDES in interpreting the results from the Pondera System and for capturing IDES requests for new functionality, data sources, and other constant improvement activities.

Upon IDES' request, Pondera will be available to review summary results of these activities with IDES on a quarterly basis. Any major issue or finding will be discussed with IDES as such major issues are discovered.

E. Pondera will provide the following hosting services for the Pondera System:

The Pondera System is hosted on the Microsoft Azure platform and data centers, which data centers physically store all physical hosting equipment, communication media, server / hardware, application access, and data storage. Pondera will provide frequent, non-intrusive updates and enhancements to the Pondera System. As a Software-as-a-Service offering, there will be frequent, non-intrusive enhancements and updates to the Pondera System. The 'What's New' tab within the Pondera System includes a description of all new functionality.

F. If required by IDES, Pondera will develop and deliver a detailed System Security Plan (SSP) prior to receipt of IDES data. The SSP documents and discusses the classification of the various data

elements obtained through IDES source files and other third-party data providers. The classification addresses the following categories:

- Public Information – Defined as information maintained by state agencies that is not exempt from disclosure under applicable state or federal laws
- Confidential information – Defined as information maintained by federal, state, and local agencies that is exempt from disclosure under applicable state or federal laws such as Personal Information, Federal Tax Information, Protected Health Information, Social Security Agency, etc.
- Sensitive information – Defined as information maintained by federal, state, or local agencies that may be public or confidential and requires a higher than normal assurance of accuracy and completeness. The key factor for sensitive information is that of integrity.

G. Pondera will provide the following data backup and recovery services for the System:

Pondera will perform encrypted file and database level backups. The encrypted backups are performed by the Azure Recovery Services Vault, are taken at the end of every business day and remain in the Azure data center. The storage system housing backup snapshots is an AES 256-bit Storage Access Network (SAN) storage device encrypted at rest. Each backup set has a pre-configured retention default period of six (6) monthly backups, five (5) weekly full backups, and six (6) daily differential backups. Once the retention period elapses, backups are overwritten.

H. Pondera will provide set up and configuration services for the System specific to IDES requirements. The System will leverage program data from IDES's own data systems. An initial output file for the previous three years will be used.

2. DELIVERABLES AND SCHEDULE OF PERFORMANCE

A. Pondera will provide the following deliverables to IDES:

1) **Master Design Document ("MDD")** – Pondera will follow the Pondera Requirements and Onboarding Process (PROP) for this project. The PROP includes structured technical and business fit-gap interviews to validate IDES requirements. The PROP is used to configure dashboard components and thresholds, and to identify IDES data sources required by FraudCaster. The result of the PROP is the MDD which will be reviewed in detail with IDES and accepted by IDES before configuration work begins. Deliverable 2(A)(2) and 2(A)(3) will also be agreed upon prior to acceptance of the MDD.

2) **System Security Plan** – Pondera will develop and deliver a SSP to govern the project. The SSP will include information on how data is transported, secured, and purged and requires sign-off by all parties prior to the transport of any data. It will also describe how data will be used and which Pondera staff will have access to data and for what purpose. The SSP shall be consistent with the terms and conditions of the Contract including, but not limited to, the confidentiality and data security requirements established under the Contract.

3) **Data Files Specifications Document** – Pondera will provide a data files specification document that details the program data required for the Pondera System implementation. This specifications document details claimant, employer, and CaseTracker level data elements and format details and includes the methodology for data utilization in the Pondera System implementation.

4) **Preliminary Leads Report** – Pondera will deliver a preliminary leads findings report from the preproduction data runs. The report will be submitted 60 days after the receipt of a complete

dataset and will include results from the claimant and employer validation components. Pondera will provide IDES with details of the data sets run and the number and types of flags that were tripped, in addition to analysis performed by the SIU.

B. This Section 2.B is an estimated project schedule for completion of deliverables identified in Section 2.A. The final schedule will be established upon a mutual agreement of the project plan.

Project Initiation:	September 15, 2020
One-Time CLEAR Batch data project begins:	September 15-22, 2020
Requirements Sessions:	September 22nd - Oct 27th, 2020
Receive Source Data:	October 15, 2020
Finalize FraudCaster Master Design Document:	November 10, 2020
Finalize CaseTracker Master Design Document:	November 24, 2020
Preliminary Leads Report:	December 17, 2020
FraudCaster & Case Tracker Go-Live:	February 22, 2021
FE Schemes/Network Analyzer Go-Live:	March 23, 2021

3. COMPENSATION AND PAYMENT TERMS

This SOW includes a 12-month subscription of the Pondera System. The first-year subscription fee is $656,329 (FraudCaster and Case Tracker) plus a one-time data run for $198,000.

A. Required Services

Solution	Annual Price
FraudCaster module subscription for up to 1.1 M claimants	$395,000
CaseTracker module subscription for up to 10 users	$167,500
SuperSearch with CLEAR ID Confirm for 1250 applicants per day	$82,125
SuperSearch with CLEAR investigations/skip tracing lookups for up to 10 users	$11,704
TOTAL SUBSCRIPTION COST	**$656,329**

Solution	Annual Price
CLEAR ID Confirm Batch **ONE-TIME** run of Claim ID's from 3/1/2020 - 9/15/2020	$198,000
ONE TIME BATCH RUN	**$198,000**

B. Renewals – The Annual Price will increase by 3% over the preceding year commencing Year 2.

4. STATEMENT OF WORK MANAGERS

The Statement of Work Managers are responsible for deliverable sign-offs and other approvals as required by this SOW. The Statement of Work Managers are:

IDES	Pondera
Thomas Revane thomas.revane@illinois.gov (312) 793-9130	Tracy Miller Tmiller@ponderasolutions.com (651) 261-0744

5. IDES RESPONSIBILITIES

The following are IDES responsibilities necessary for Pondera to provide the Services described in this SOW in a timely manner as mutually agreed upon by the Parties:

- IDES will provide technical user participation during the PROP to help Pondera identify and transfer data from source data systems.
- Throughout the implementation of the Pondera System, IDES will provide Pondera access to technical staff to respond to questions about database schemas, column names, and other technical aspects of IDES source data.
- IDES will produce the data extracts that Pondera will cleanse and transform for use in CaseTracker.
- IDES will provide master employer files including data elements such as name, address, Internal Unique ID type, etc.. All required specifications are included in the Pondera Data File Specifications Document.
- IDES will provide initial claims, continuing claims, and PUA claims information for the past three (3) years.
- IDES will provide weekly certification information for the past three (3) years.
- IDES will provide unemployment insurance tax information including, employer info, employer UI tax rate, inactive employers, NAICS codes, etc. for the past three (3) years.
- IDES will provide Master Claimant File including data elements such as name, SSN, DOB, ID number, etc. All required specifications are included in the Pondera Data File Specifications Document.
- IDES will provide data dictionaries from all data systems that will feed employer, claimant, and claims data delivered to Pondera.
- IDES will provide functional user participation during the onboarding sessions to validate requirements, work on thresholds, configure reports and other system functions, identify sources of IDES data for the analytics, and approve deliverables.
- IDES will provide functional user participation in quarterly meetings to review the results of the analytics, user statistics, and new data sources and system functions.

6. ASSUMPTIONS

Pondera makes the following assumptions applicable to this SOW:

- Pondera will comply with the security, data use, and confidentiality requirements established under the Contract and SSP when signed by both parties; and
- All project timelines are based upon the identified delivery timelines for program data and technical/program feedback. Any delay in the delivery of the data or responses to clarifying questions surrounding the configuration of the data for FraudCaster, will result in delays to the proposed implementation schedule and may result in a Change Order.

Agreed to and accepted by:

Pondera Solutions, LLC

By: [redacted]

Printed: [redacted]

Title: Sr. Vice President

Date: 09/10/20

Illinois Department of Employment Security (IDES)

By: [redacted]

Printed: Kristin A. Richards

Title: Acting Director

Date: 9/11/20

Attachment II

OVERVIEW OF PONDERA FRAUD DETECTION & CASE MANAGEMENT

PONDERA
PART OF THOMSON REUTERS

80 Blue Ravine, Suite 250
Folsom, CA 95630

Point of Contact:
Caryn Otto
cotto@ponderasolutions.com
916.607.4131

TABLE OF CONTENTS

INTRODUCTION

Since its inception in 2011, Pondera Solutions LLC's (Pondera) sole focus has been detecting, preventing, and investigating fraud, waste, and abuse (FWA) in large government programs, including unemployment insurance, social services, and health care.

In March of this year, Thomson Reuters acquired Pondera, combining the industry's best public records data (CLEAR®)and Pondera's leading fraud analytics and case management platform. This combination allows us to offer governments the most powerful solution to combat fraud, waste, and abuse in the unemployment insurance program.

For the Illinois Department of Employment Security's (IDES) program integrity efforts, we bring:

FraudCaster®, an existing, configurable fraud detection and prevention solution

- Integrated investigative case management (CaseTracker™) collectively with FraudCaster is referred to as the "System")
- ID Confirm and CLEAR data options, with over 60 data sources and billions of records
- Experienced SIU staff with unemployment insurance program integrity expertise
- A proven implementation methodology to tune your System with IDES' unique requirements

PROPOSED SOLUTION

Pondera's sophisticated System identifies fraud schemes in unemployment insurance. IDES investigators can simply log-in to the FraudCaster dashboard to view results from advanced analytics, rules, and third-party data crossmatches, and can quickly validate leads and convert them into cases, using our integrated CaseTracker.

FraudCaster generates alerts on UI claimants and employers for wage conflicts, SUTA dumping, worker misclassification, identity theft, deaths, incarceration, and many other program or behavioral violations.

In 2018, a UI client achieved $5,973,515 in return on investment (8.5X ROI) with Pondera's System. This client had 2,508 cases opened and 2,268 cases closed. Since the deployment of CaseTracker in February 2016 through December 2018, this client achieved $16,357,884 in program savings. Additionally, current leads identified by their Pondera System are averaging 4:1 improvement on identified recovery dollars versus non-Pondera System identified leads.

FraudCaster

FraudCaster is an advanced fraud, waste, and abuse detection and prevention solution. [redacted]

FraudCaster includes dozens of pre-configured UI alerts, clusters, trends, and models for IDES investigators.

Alert types include identity theft, wage conflicts, SUTA dumping, worker misclassification, fictitious employer, and fictitious employee schemes. The dashboard also includes visualizations depicting IP, address, phone, and bank account sharing.

FraudCaster then displays its results via an intuitive dashboard (shown in Figure 1) that includes configurable alerts, interactive geospatial maps, and profiles for entities. Once in production, Pondera schedules regular data feeds from program systems and returns validity scores and investigation recommendations to the dashboard. FraudCaster's current alert library includes dozens of unemployment insurance specific rules.

Figure 1: The FraudCaster Dashboard

FraudCaster also analyzes referrals and cases using Thomson Reuters CLEAR and other relevant pre-integrated third-party data sets for both businesses and individuals. CLEAR provides access to billions of additional records about claimants and employers for analytics and reporting. In addition, Pondera will integrate up to five (5) state data sources such as the NDNH database, DMV records, incarceration records, and other desired sources.

FraudCaster is a force multiplier for any program integrity unit. With limited resources and a constant influx of new referrals, IDES managers and investigators will leverage FraudCaster's analytics to understand claimant and employer risk as well identify prior behaviors and patterns of fraudulent behavior. This leads to the assignment and prioritization of the true highest value cases.

Scorecard

FraudCaster is designed to triage leads based on their fraud risk scores. Consequently, an important differentiator for Pondera is our Scorecard functionality. The Scorecard combines information from all the data sources and streams, in addition to violations generated by FraudCaster, and generates a fraud risk score from 1-100, for likelihood of FWA (shown in Figure 2), for every program participant. Scorecards are especially effective for programs with large numbers of participants. FraudCaster will likely generate thousands of flags with each new data run. The Scorecards bring clarity to the large number of program violations, allowing users to detect the most egregious violators.

Figure 2: The Scorecard ranks all program facilities based on their fraud risk score

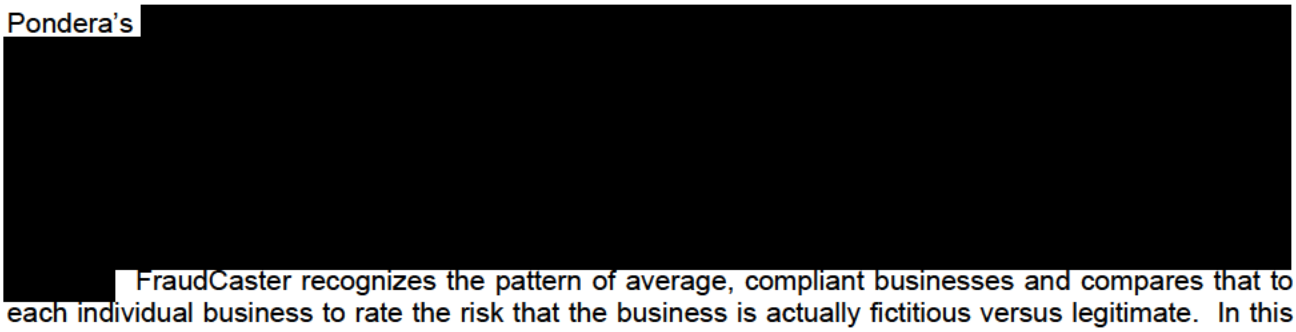
The result is a quicker, more efficient investigative process that aids in the detection and investigation of the program's greatest integrity threats. Pondera's learning algorithms further aid in providing critical information on areas of program vulnerability to inform and improve policy and procedures, thereby reducing future instances of improper payments.

Fictitious Employer (FE) Scheme Visualizer

Pondera knows from experience that not all employers properly register and comply with their reporting responsibilities. FraudCaster uses data and algorithms to identify businesses that are not in compliance, including:

- Those known to have employees but are not registered
- Registered businesses that do not report all of their employees
- Registered businesses that have related businesses, allowing them to "move employees" from one business to another in an effort to reduce their required unemployment contribution rate
- Fraudsters who register a fictitious business and fictitious employees in an effort to defraud the State's unemployment system

Pondera's



FraudCaster recognizes the pattern of average, compliant businesses and compares that to each individual business to rate the risk that the business is actually fictitious versus legitimate. In this example, the employer scammed a State UI program out of $149K of taxpayer money over a one-year period.

Figure 3 : FE Scheme Visualizer Example

FraudCaster will be configured specifically for the IDES, including alerts, geospatial maps, and profiles with fraud indicators. Pondera will leverage claimant and employer data from IDES's own data systems. For this implementation, an initial output file for the previous three years is recommended.

The base FraudCaster functionality is extended to all users (unlimited IDES users permitted). We continue to work with you after the initial go live to identify new alerts and functionality to develop and push into IDES's System.

Pondera will deliver a software subscription of FraudCaster with the functionality identified in Table 1.

Table 1: FraudCaster Base Functionality

Activity	Description	Quantity
Claimant Validation		Up to 1,100,000 claimants
Employer Validation		Up to 375,000 Profiles
Procedural Flagging		Up to 20 flags
Geospatial Analysis		Up to 3 maps
Street View		Up to 1,500,000 Entities

Activity	Description	Quantity
Data Matching	[redacted]	Up to 1,500,000
Scorecard	[redacted]	1 Claimant Scorecard

The functions described in Table 1 will detect and flag anomalous and suspect activity. In addition, they will help identify high-risk groups of claimants and employers.

CaseTracker

The sheer volume of referrals that IDES assesses and investigates annually necessitates a mechanism to intake, assess, assign, and monitor referrals as they move through the investigative life cycle. Moreover, the scope and level of complexity associated with IDES cases, further demands tools to manage the investigative process (including reports of interview, documents collected, case actors, time and expense tracking, etc.) to maximize efficiency.

Pondera's CaseTracker is a fully integrated investigative case tracking and management system. CaseTracker includes robust reporting capabilities to view caseloads, progress, and statistics on case resolution times. IDES users can leverage all data captured within the CaseTracker module to easily run queries and ad-hoc reports. The module includes a fully integrated business intelligence tool that allows for individualized reporting for each user based on any information captured. Users can easily create reports using a drag-and-drop interface and can save them to their dashboard for future use.

The reporting tool is used to aggregate any case data to create customizable reports for external consumption. Reports can automatically be broadcast to PDF, CSV, DOC, XLS, Word, or HTML. Standard reports, including the ROI report below (Figure 5), display information on numbers of cases assigned to investigators, average time to completion, and other common reporting metrics.

Figure 4: CaseTracker includes standard reports like this ROI Report.

Moreover, the System supports and fosters the accurate and complete documentation of investigative work through data validity business rules. For example, if the user attempts to save and move the case forward without any required fields (identified with a red asterisk) populated, the user interface provides an error message that prompts the user to correct the missing field(s) before moving forward. This is essential to ensuring the System delivers clear and accurate reports.

Pondera will deliver a software subscription of CaseTracker for up to 15 users with the functionality described in Table 2.

Table 2: Proposed Case Management Functions

Function	Description	Max Annual Quantity
Intake Form	The intake form is used to record new cases.	1
Workflow	Workflow rules are used to optimize the business process. A 'rule' islogic that triggers a change in status.	Up to 7
Case Record	The case record will contain all the standard case functionality including those items in Case Details section.	No limit
Case Details Overview	This tab displays information on the intake form and includes up to 150 fields (closure reason, recommended outcome, etc.).	No limit
Case Activity	• Record Notes	No limit

Function	Description	Max Annual Quantity
	• Record To-Do's with reminders • Assign To-Do's to a CaseTracker user other than case owner • Send and receive emails from within a case.	
Case Entities	Add multiple entities to a case to record various 'Entity Types' (i.e. customer, subject, witness, etc.). Each of the unique forms may have up to 50 data fields.	Up to 3
Case Files	Attach any sort of electronic document to the case (fax, scanned document, MS Word, etc.) with a maximum individual attachment size of 200 MB.	No limit
General Case Features	Ability to assign a case by selecting an owner from the pick list and the ability to print the case file. There is also case history that will display an audit trail of changes made to the case record.	No limit
Integration with Current System	Pondera can import cases from the existing case management system. Many clients choose to import active cases only.	No limit
Case Record Forms	Forms can be deployed within the case file to record information. Forms are used for data sets that must be recorded more than once during the case lifecycle. For example: An expense form could be deployed to track many expense items. An interview form could be deployed to record every interview conducted.	Up to 7
Maintenance	Pondera provides the following maintenance functions: • Add, modify or delete users, select their access level and notify them by email of their username and password • Add, modify or delete category items (issues, products, etc.) • Add, modify or delete workflow rules (for example: users may change timing of notifications) • Add, modify or delete email standard responses	No limit
Access Controls	Access controls restrict functions and data available to groups of users. For example, information may be restricted based on the user's department. In that case, the user only sees cases and report information related to that department. Other examples could include case type, location, severity, etc.	Up to 5 roles
Reporting	CaseTracker includes a standard reporting package. This is an ad-hoc reporting tool integrated in case management and will be populated with reportable field values. Pondera will provide reports based on the IDES requirements, such as audit or investigation outcomes, progress of prosecution referrals and hearings, and performance, to monitor program integrity efforts.	Up to 7 pre-configured reports and 4 ad-hoc reporting licenses
Automated steps	Built in processes to allow users to configure specific functions including transferring a complaint to a case, case assignment, set notifications for updates related to records submissions, reporting dates, field population, dependencies, form indicators etc.	Up to 8 business rules
Search options on Advanced Search and Case View	Ability to search within CaseTracker to identify potentially related cases or providers.	Up to 5 search criteria
Time & Expense Tracking	CaseTracker includes a standard employee time and case expense tracking functionality. This facilitates the seamless creation of employee routine timesheets and investigative costs.	No limit

Thomson Reuters CLEAR & CLEAR ID Confirm Batch

We leverage and integrate Thomson Reuters CLEAR database, which pulls from over 60 data sources to provide IDES access to billions of additional records about employers and claimants for analytics and reporting. These sources include individual and business records, identity information, criminal backgrounds, incarcerations, deceased status, best known address, affiliates, linkages, social media, and more.

Thomson Reuters CLEAR helps more than 14,000 agencies at all levels of government through its aggregation of billions of public records powered by cutting-edge technology that allows customers to identify the most recent and accurate information about people and companies.

CLEAR ID Confirm Batch integrated with FraudCaster

[redacted]

- Discover new data to know whether the subject is who they say they are
- Compare information provided against continuously updated records
- Immediately identify possible fraudulent IDs with identity flags
- Analyze all of the identities related to claims since 3/1/2020 data.

CLEAR Investigative Look-ups

CLEAR Online Lookup provides comprehensive and current data sources, functionality, and exclusive offerings that comprise the most comprehensive investigative platform available. CLEAR increases the efficiency and the effectiveness of due diligence and investigations by providing:

- An easy-to-use online interface with dashboard presentation of results, including display with investigative tools such as Quick Analysis Flags and Address Map
- Access to vast collections of public records, publicly available information [redacted]
- [redacted]
- Access to Web information, such as social networking sites, blogs, and news

CLEAR for Skip Tracing

CLEAR for Skip Tracing includes the data sources, functionality, and exclusive offerings to provide a fast, efficient means of locating and verifying information on individuals:

- An easy-to-use online interface with dashboard presentation of results, including a display with investigative, dashboard tools such as Associate Analytics and Address Map
- Live gateway data available directly from the Contact View (Figure 5), specifically designed to meet skip-tracing needs
- Enhanced phone content includes consumer phone records in the hundreds of millions
- Reverse cell phone lookup and VoIP data
- Utility data—updated daily—often divulges locate information otherwise unpublished or unknown
- Death indicators that verify if a debtor has passed away

- Asset, licenses, and potentially adverse information are filtered, allowing users to focus on find and locate information
- Reports available when a deeper dive is needed

Figure 5 is a close-up of the Contact View which shows the convenient summary of vital information—including best address and best phone—that is immediately available after running a search, without having to run a report.

Figure 5: Skip Tracing lookup information

IMPLEMENTATION & DELIVERABLES

We implement and configure the System using the Pondera Requirements and Onboarding Process (PROP). The PROP is an interactive process that validates existing requirements, uncovers new and possibly unknown requirements, gathers information for threshold and model tuning, and assesses training needs. Typical implementation timeline is three to four months from receipt of data.

The PROP contains six main steps, as highlighted below. In addition, project management, infrastructure, and training work streams run throughout to support the following PROP process:

- **Step 1: Plan** – During this step, the project management framework will be developed and deployed including validation of the detailed project schedule, development of customer deliverables, and development of the project management plan, including communications and change management plans. The project kick-off meeting marks the end of the project planning step.
- **Step 2: Fit Gap** – Key participants will be identified, and a schedule developed for structured interactive discussions. Structured interactive discussions will occur by topic to validate functional and technical requirements and determine the fit gap with the Pondera System. These decisions will be documented in a Master Design Document.
- **Step 3: Build** – During this step, we configure the System based on the decisions made during the Fit Gap step (Step 2) including adjustment of the thresholds for COTS reports. If needed, we hold additional program and policy sessions to fine tune the solution. Features that are not out-of-the-box will be developed during this step. Finally, we send source data through a rigorous QA process.
- **Step 4: Test** – During this step, Pondera executes numerous levels of tests including analytics output validation/quality assurance, smoke tests, unit tests, impact analysis tests, and user acceptance demonstrations. This results in a solution with functionality that has been validated and approved by the customer.
- **Step 5: Deploy** – During this step, we deploy functionality to production, train end users, and the System will go live.
- **Step 6: Operations** – During this step, Pondera will provide post-production support including statistical support, help desk support, post implementation reviews, and configuration management to fine tune the models. In Operations, the System is fully functional.

Pondera will provide the following deliverables for this implementation:

- **Requirements Validation** – Pondera will conduct structured technical and business fit-gap interviews to validate IDES requirements.
- **Security Plan** – Pondera will develop a System Security Plan (SSP) to govern this project. The SSP will include information on how data is transported, secured, and purged. It will also describe how data will be used in crossmatches and which Pondera staff will have access to data and for what purpose.
- **Production System** – Pondera will configure and deploy the System with the functionality described in Tables 1 and 2 and based on the results of the PROP sessions. Pondera will provide hosting services and store and process data in the secure, FedRAMP High certified Microsoft Azure environment.
- **User Training** – Prior to go live, Pondera will conduct on-site training for IDES management and staff using the production System. Pondera will provide one management session and up to three staff sessions. Additionally, we will provide ongoing training refreshers, as needed (remote). Pondera will conduct the training and provide all required course materials.
- **Post-Implementation Support** – Pondera will provide post-implementation technical and user support as needed. In addition, Pondera's Special Investigations Unit (SIU) will be available to assist in case development for high profile cases. Case support includes dedicated analysts, data analysis, link analysis, and findings reports. It is also important to note that with our Software-as-a-Service

System models, features, and functions are added on a regular basis as part of your annual subscription fee. Figure 6 details the overall system architecture.

Figure 6: FraudCaster System Architecture