ADOA-ASET

Project Investment Justification

Version 03.31.15

A Statewide Standard Document for Information Technology Projects

Project Title:

PRIVATE FRAUD PREVENTION INVESTIGATION SERVICES

Agency Name:	Arizona Department of Revenue
Date:	July 17, 2015 revised November 10, 2015
Agency Contact Name:	Roxanna Rodriguez
Agency Contact Phone:	(602) 716-6080
Agency Contact Email:	rrodriguez@azdor.gov

Hover for Instructions

I. Project Investment Justification (PIJ) Type*

☐ Yes ☒ No Is this document being provided for a Pre-PIJ / Assessment phase?

If Yes,

Identify any cost to be incurred during the Assessment phase.	$
Based on research done to date, provide a high-level estimate or range of development costs anticipated for the full PIJ.	$

Explain:

Click here to enter text.

☐ Yes ☒ No Will a Request for Proposal (RFP) be issued as part of the Pre-PIJ or PIJ?

II. Business Case

A. *Business Problem**

Over the past decade, financial institutions, including the Internal Revenue Service (IRS) and state agencies, have become targets for very high stakes financial crimes. State tax agencies, including the Arizona Department of Revenue (ADOR) and the IRS have been affected by a particular scheme in which false individual income tax returns are filed under false names and social security numbers, with fraudulent W-2 forms. Perpetrators include individuals, fraud rings and dishonest tax preparers. While the increasing reliance on e-filing for tax returns has increased the efficiency of tax operations and taxpayer convenience, the reliance on e-filing has also opened opportunities for fraud on a larger and more sophisticated scale than before.

In 2013, as a measure to supplement the work of the existing Fraud Detection Team under the Criminal Investigation Unit (CIU), the ADOR established a Fraud Task Force to determine what additional steps could be implemented to address the issue of fraudulent income tax returns. Fraud Task Force members were able to enhance fraud identification criteria utilizing data that was available both in-house and externally.

The Criminal Investigation & Fraud Detection staff was able to stop over $31.8 million in fraudulent refunds for fiscal year 2013 and over $73.8 million in fiscal year 2014. Despite their success, there remain challenges and opportunities in order to improve the detection and investigation process of high-risk and fraudulent returns.

Currently, the process used by the department to identify fraudulent tax returns is labor intensive and utilizes resources from other divisions of revenue. These resources would normally be revenue generating positions within the department.

The objective is to stop fraudulent income tax refunds in the early stages of processing. Early detection of fraud limits the waste of resources, and allows higher levels of efficiency and accuracy. It is recommended to automate as many of the business rules and fraud detection as possible.

B.   *Proposed Business Solution**

The proposed business solution is to acquire a Commercial off the Shelf (COTS) modernized identity verification and fraud prevention solution that consists of predictive analytics, modeling and ad hoc data mining of internal and external data sources.

The vendor shall provide a comprehensive solution, housed by the State, which includes all hardware, software, security, installation services, user training, and 24X7 help desk support.

C.   *Quantified Benefits**

X	Service enhancement
	Increased revenue
X	Cost reduction
X	Problem avoidance
X	Risk avoidance

Explain:

Improvement	Description
Manual Process	Improved data, additional criteria and an increase in the automation process enhances efficiency and decreases time consuming research, potentially reducing the necessity of assigning and/or hiring additional auditors for the Fraud Detection Team during tax season.
Threshold Enhancement	Technological support for the identification of fraudulent income tax returns allows refund requests to be examined for potential fraud.
Investigative Resources	Availability of enhanced and up-to-date identity verification information reduces the number of false positives, thus increasing ADOR's ability to determine whether or not a return is fraudulent without human intervention.
Technology Needs	Currently, necessary manual research requires more powerful workstations, servers, and utilization of larger dual monitors systems. Additionally, while researching potential fraud cases, Fraud Detection Team staff must frequently open and close multiple applications. Mechanization of the fraud identification process potentially reduces the immediate need for additional computer hardware for fraud analysis staff.
Strategic Priorities	Benefits of the aforementioned improvements are in line with the following ADOR's 2015 strategic priorities:

- Modernization and Sustaining Core Processes
    - o   Process Improvement and Modernization
- Process Efficiencies and Lean
    - o   Increased Process Efficiencies
    - o   Cyber Crimes

III. Technology Approach

A. *Proposed Technology Solution**

The proposed technology solution will provide an analytic warehouse on a secure platform. The solution will utilize high speed servers and database technology to increase investigative efficiency through the use of data, modeling and predictive analytics. Furthermore, the solution will validate identities, detect suspicious returns, identify fraud and recognize emerging fraud trends.

The vendor will install and maintain all hardware, software and data products with minimal impact to ADOR resources.

B. *Existing Technology Environment*

In its entirety, ADOR's current technology consists of the Accenture BRITS system, also known as the Tax Administration System (TAS). It is a multi-platform and multi-database system. Currently, income tax returns are electronically filed (Me-File) or submitted via paper forms. The paper forms are entered into TAS through data entry methods or if they contain a barcode (2-D), scanned into the system.

Once in the TAS system, the income tax returns are analyzed as part of the fraud prevention and identification process. If the return is suspected of being fraudulent, the return is placed in a suspense file for further review by the Fraud Detection Team. If no fraud is found, the return posts to TAS and the refund is released.

C. *Selection Process*

The ADOR Audit staff contacted several states to inquire about their approach to the current problem of identity theft and the filing of fraudulent individual income tax returns. Many states use more than one method to combat this problem from physically reviewing tax returns, preforming various analytics, to scoring of returns by outside vendors and sending questionnaires to taxpayers to verify their identity. It was also inquired as to whether or not these systems were purchased or built in-house.

Per statute, ADOR must make a Request for Proposal (RFP) and review all outside vendor submissions prior to awarding a contract for services. ADOR issued a solicitation and received and reviewed various responses. After reviewing the proposals, the Department completed an evaluation and selected an approach that would be suitable for improving the process for the detection of fraudulent individual income tax returns. The evaluation criteria consisted of methodology, capacity to offer/experience and cost. An award is being proposed based on the most advantageous proposal to the State.

IV. Project Approach

A. *Project Schedule**

Project Start Date: 8/31/2015   **Project End Date:** 2/1/2016

B.   Project Milestones

Major Milestones	Start Date	Finish Date
RFP Process	8/31/15	11/06/15
ITAC Presentation	11/18/15	11/18/15
Bid awarded to vendor	11/18/15	11/19/15
Project Charter	11/06/15	11/18/15
Technology Architecture	11/06/15	11/18/15
Installation and Configuration	11/23/15	12/11/15
Software Configuration and Deployment	12/11/15	01/08/16
Testing of Software	01/11/16	01/15/16
Training of Staff	01/18/16	01/22/15
User Acceptance – Application / Methodology	01/25/16	01/27/16
User Acceptance – Reporting Results	01/28/16	01/29/16
Release Project Resources	01/29/16	01/29/16
Project Closeout	02/01/16	02/01/16

C.   Project Roles and Responsibilities

Role	Responsibilities
Business Owner and Sponsor	- Ultimate decision-maker and tie-breaker - Provide project oversight and guidance - Review/approve project elements - Approve resource allocation strategies, and significant changes to resource allocation - Resolve conflicts and issues - Review deliverables
ADOR Project Manager	- Manage projects in accordance to the appropriate methodology or framework - Communicate and coordinate with outside vendors - Manage the project progress of outside vendors - Serve as SME to the sponsor(s) - Complete project charter - Receive direction and guidance from the sponsors - Provide regular updates to sponsors - Provide overall project direction - Direct/lead team members toward project objectives
ADOR Criminal Civil Investigations, Information Technology Division, Administrative Services Division, Process Administration and Audit Divisions Subject Matter Experts	- Complete assigned tasks - Lend expertise and guidance as needed - Understand the user needs and business processes of their area - Act as consumer advocate in representing their area - Communicate project goals, status and progress throughout the project to personnel in their area - Review and approve deliverables - Provide knowledge and recommendations - Helps identify and remove barriers - Assure quality of deliverables that will met the project goals and objectives - Identify risks and issues and help in resolutions - Product acquisition
ADOR Information Technology Division	- Identify risks and issues and assist with resolutions - Completes site visit if required - Information security

ADOA Information Technology Divisions	▪ Identify risks and issues and help in resolutions ▪ Product acquisition ▪ Information security
Vendor	▪ Identify risks and issues and help in resolutions ▪ Technological demonstration and instruction ▪ Provide necessary hardware and software ▪ Software interface ▪ Information security

V. Risk Matrix, Areas of Impact, Itemized List, PIJ Financials

RV16001
PIJ-FINANCIALS 151C

VI. Project Approvals

A. Agency CIO/ISO Review and Initials Required*

Key Management Information	Yes	No	Inits
1. Is this project for a mission-critical application system?	X		
2. Is this project referenced in your agency's Strategic IT Plan?	X		
3. Have you reviewed and is this project in compliance with all applicable Statewide policies and standards for network, security, platform, software/application, and/or data/information located at https://aset.az.gov/resources/psp? If **NO**, explain in detail in section **"VIII. Additional Information"** below.	X		
4. Will any PII, PHI, or other Protected Information as defined in the 8110 Statewide Data Classification Policy located at https://aset.az.gov/resources/psp be transmitted, stored, or processed with this project? If **YES**, the **Protected Data** section under **"VII. Security Controls"** below will need to be completed.	X		
5. Will this project migrate, transmit, or store data outside of the agency's in-house environment or the State Data Center? If **YES**, the **Hosted Data section** under **"VII. Security Controls"** below will need to be completed.		X	
6. Is this project in compliance with the Arizona Revised Statutes and GRRC rules?	X		
7. Is this project in compliance with the Statewide policy regarding the accessibility to equipment and information technology for citizens with disabilities?	X		

B. Project Values*

The following table should be populated with summary information from other sections of the PIJ.

Description	Section	Number or Cost
Assessment Cost (if applicable for Pre-PIJ)	I. PIJ Type - Pre-PIJ Assessment Cost	$0.00
Total Development Cost	V. PIJ Financials tab	$1,060,000 to $5,300,000
Total Project Cost	V. PIJ Financials tab	$2,225,000 to $13,785,000
FTE Hours	See Hover text for FTE Hours	1500

C. Agency Approvals*

Approver	Printed Name	Signature	Email and Phone
Project Manager:	Vivek Chaudhary		vchaudhary@azdor.gov (602) 716-6408
Agency Information Security Officer:	Johnathon Edwards		jedwards@azdor.gov (602) 716-6145
Agency Acting CIO:	Johnathon Edwards		jedwards@azdor.gov (602) 716-6145
Project Sponsor:	Anthony Forschino		aforschino@azdor.gov (602) 716-6921
Agency Director:	David Briant		dbriant@azdor.gov (602) 716-6918

VII.   Security Controls

Collaboration with the ADOA-ASET Security, Privacy and Risk (SPR) team may be needed to complete this section, which is only required for those projects that involve data that is Protected or Hosted outside of the Agency or State Data Center. Additional information can be found in the NIST FRAMEWORK section under RESOURCES at https://aset.az.gov/resources/psp or you may wish to contact ASET-SPR directly at secadm@azdoa.gov for assistance.

A.   *Protected Data*

All data for this project is considered "Protected Data" under statewide policy 8110. This data could contain federal taxpayer information and shall comply with the Federal classification authority and Federal protection requirements.

All network-transmitted data sent to, from, and through the system will be protected through use of the following best-practice security designs:

- ➢ The vendor will use industry-standard message specifications and formats for communications with external applications. Business services use standard parameters encoded in binary format.
- ➢ Windows Communication Foundation (WCF) message-level encryption algorithms will be enabled in accordance with agency security policies.
- ➢ The vendor will encrypt the data in transit within an agency's network. Standard SSL encryption in the browser is used for messaging between client workstations and web services.
- ➢ Message data is signed and encrypted using SSL for external communication or for internal WCF messages.
- ➢ Inbound messages will be validated for allowable data to prevent compromising content.
- ➢ Message attachments will be scanned at the server using standard server-based virus scanning software.
- ➢ Communication between the application and database servers will be encrypted using SSL certificates.
- ➢ All data shall be encrypted at rest and in transit
- ➢ The Vendor shall provide security controls to protect the data as defined in the current revision of the National Institute of Standards and Technology (NIST) Special Publications (SP).
- ➢ The Vendor must complete and provide to ADAO-ASET SPR the Arizona Baseline Security controls document referenced above.

For greater security, "at-rest" data in SQL Server 2012 (such as data files, temporary database files, and log files) will be encrypted using the Transparent Data Encryption (TDE) capabilities in Microsoft SQL Server.

B.   *Hosted Data*

☐   Check here if the https://aset.az.gov/arizona-baseline-security-controls-excel

spreadsheet is attached. Otherwise explain below what information/ support is needed to complete the spreadsheet and/or why no sheet is attached:

The solution will not be hosted by the vendor, but within the State data center. The AZ Baseline Security Controls spreadsheet is available and will be provided upon request.

☐ Check here if a Conceptual Design / Network Diagram is attached. Otherwise explain below what information/support is needed to complete the diagram and/or why no diagram is attached:

This Conceptual Design Diagram is available and will be provided upon request.

VIII.   Additional Information

IX.   Attachments

The following are examples of supporting documents that should be sent as email attachments when required:

A.   *Vendor Quotes*
B.   *Arizona Baseline Security Controls spreadsheet*
C.   *Conceptual Design / Network Diagram*
D.   *Other*

X.   Glossary

Other Links:
ADOA-ASET Website
ADOA-ASET Project Investment Justification Information Templates and Contacts

Email Addresses:
Strategic Oversight
ADOA-ASET_Webmaster@azdoa.gov

ADOA-ASET - Arizona Strategic Enterprise Technology
Project Investment Justification - Risk Matrix

Project ID: | To Be Provided by ADOA-ASET | Date Accepted: | To be Provided by ADOA-ASET

Project Information

Agency Name	Project Name	Date Submitted
Arizona Department of Revenue	Private Fraud Prevention Investigation Services	10/27/15

Project Questions	Agency Response (Y/N)
Does the project involve customized software not previously implemented by your agency?	N
Does the project involve a customized application not previously developed by your agency?	N
Does the project involve any technology that is new and/or unfamiliar to your agency?	Y
Does the project involve multi-agency and/or multiple vendor coordination?	N
Is there any possibility that project implementation costs could reach $1 million or more? (Include professional services, hardware, software, license fees, taxes, shipping, etc.)	Y
Will the project require that a Request for Proposal (RFP) be issued?	Y
Are there any known schedule or budget constraints?	Y
Does this system interface among 2 or more applications?	Y
Will the implementation involve major end user view or functionality changes?	N
Will the implementation require any physical infrastructure improvements, e.g., building reconstruction, etc.?	N
Are there other high risk project items not identified? If so, please explain below:	N
Does the project fall into one of the following categories: - hardware technology refresh, e.g., PCs, laptops, radios, peripherals, etc.? - software version refresh, e.g., MS Office 2010 replacing 2007? - enhancements to an existing application, e.g., web app, internal system?	N
Will the technology and all required services be acquired off existing State contract(s)?	N
Does the project have the correct skillset and number of in-house resources assigned to meet the objectives?	Y
Will a dedicated Project Manager (PM) be assigned?	Y
Will the PM managing the project be credentialed (if costs could reach $1 million or more)?	Y
Does your agency have experience with the vendor (if used)?	N
Does the vendor have professional experience with similar projects?	Y

Investment Sustainability Questions	Agency Response (Y/N)
Are ongoing/5-year support costs, once the project has been implemented, reflected in the operational costs for the PIJ?	Y
Has your agency addressed supporting components to ensure the investment can be sustained, e.g., documentation, application ownership, portability, plans upon contract/support termination?	Y
Does the production site have suffecient failover and disaster recovery plans in place to assure your agency will be able to recover from an unplanned incident?	Y
Does your agency and/or the proposed vendor have the resources and supporting infrastructure currently in place to sustain the proposed investment?	Y

Agency Questions	Agency Response (Y/N)
Are all current agency projects in "Green" status, with no outstanding issues that ADOA-ASET is monitoring?	N
Does your agency currently have any projects that are in "Red" status?	Y
Has your agency demonstrated a consistent reporting relationship with ADOA-ASET Oversight, e.g. reports submitted on time and accurate (verified by CIO)?	Y
Is this your agency's first PIJ?	N
Has it been more than 2 years since your agency submitted a PIJ?	N
Does your agency have a formal project methodology in place?	Y

ADOA-ASET - Arizona Strategic Enterprise Technology
Areas of Impact

Please check which of the following technology areas will be included in the proposed solution - check all that apply:

Application Systems
- [ ] Application Enhancements
- [ ] Internal Use Web Application
- [ ] Mobile Application Development
- [ ] Arizona Enterprise Solution Platform (AESP) based Application
- [ ] New Application Development
- [ ] az.gov Web Portal

Database Systems
- [x] Data Warehouse/Mart
- [x] Database Consolidation/Migration/Extract Transform and Load Data
- [x] Database Products and Tools
  - [x] Oracle
  - [ ] DB2
  - [ ] Other: (Please specify below)
  - [ ] MySQL
  - [x] MS SQL Server

Software
- [x] COTS Application Acquisition
- [ ] Mainframe Systems Software
- [ ] Open Source
- [ ] Other: (Please specify below)
- [ ] COTS Application Customization
- [ ] PC/LAN Systems Software
- [ ] Virtualization

Hardware
- [ ] LAN/WAN Infrastructure
- [ ] Mainframe Infrastructure
- [ ] Storage Area Network Devices
- [ ] Public Safety Radios, Systems
- [x] Other: (Please specify below)
- [ ] PC Purchases, Peripherals
- [ ] Tape Libraries/Silos
- [ ] UPS Devices

Vendor provided servers

Hosted Solution (Cloud Implementation)
- [ ] State Data Center
- [ ] Commercially Hosted
  - [ ] Amazon (AWS) GovCloud
  - [ ] Century Link - I/O Data Center
  - [ ] AWS (non-government) cloud
  - [ ] Microsoft Azure
- [ ] Vendor Hosted
- [ ] Other: (Please explain below)

N/A

Security

- ☐ Encryption
- ☐ Security Appliances
  - ☐ Firewall
  - ☐ Intrusion Detection System (IDS)
  - ☐ Intrusion Prevention System (IPS)
  - ☐ Other: (Please specify below)
- ☐ SecurityControls/Systems - Other: (Please specify below)
- ☐ Physical Controls (Badging Systems, Iris Scanners, Other: (Please specify below)

Telecommunications

- ☐ Network Communications Infrastructure
- ☐ Telephone Upgrade-Business-Specific
- ☐ Cabling
- ☐ Wireless Access Points
- ☐ Telephony Upgrade-EIC Solution
- ☐ Trenching
- ☐ Videoconferencing
- ☐ Other: (Please specify below)

Enterprise Solutions

- ☐ Business Intelligence System
- ☐ E-Signatures
- ☐ Geographic Information Systems
- ☐ Other Imaging - Photos, Fingerprints, etc.
- ☐ Document Management/Imaging
- ☐ eLicensing
- ☐ Management Systems - Financial, Grants, Asset
- ☐ Disaster Recovery/Business Continuity
- ☐ Other: (Please specify below)

Contract Services/Procurement

- ☐ Contract Project Management
- ☐ Contractor Support Services
- ☐ Install/Configuration Contract Services
- ☐ State Contract
- ☐ Vendor provided
- ☑ Procurement (RFP, IFB, DPR, etc.)
- ☐ Other: (Please explain below)

ADOA-ASET - Arizona Strategic Enterprise Technology
Project Investment Justification - Itemized List

Project ID: | To Be Provided by ADOA-ASET | Date Accepted: | To be Provided by ADOA-ASET

Project Information

Project Name	Agency Name	Date Submitted
Private Fraud Prevention Investigation Services	Arizona Department of Revenue	10/27/15

Project Cost - Itemized

Item	Description	Category	Development or Operational	Qty or Hours	Unit Cost	Tax (if app)	Extended Cost
1	Hardware, software, data, and all associated development	Other	Development	1	$1,060,000 to $5,300,000	$0.00	$1,060,000 to $5,300,000
2	Ongoing operaational expenses, maintenance, support	Other	Operational	4	$228,750 to $2,058,750	$0.00	$915,000 to $8,235,000
3	Support Services	Prof & Outside Services	Operational	1	$250,000.00	$0.00	$250,000.00
4		[--Select--]	[--Select--]			$0.00	$0.00
5		[--Select--]	[--Select--]			$0.00	$0.00
6		[--Select--]	[--Select--]			$0.00	$0.00
7		[--Select--]	[--Select--]			$0.00	$0.00
8		[--Select--]	[--Select--]			$0.00	$0.00
9		[--Select--]	[--Select--]			$0.00	$0.00
10		[--Select--]	[--Select--]			$0.00	$0.00
11		[--Select--]	[--Select--]			$0.00	$0.00
12		[--Select--]	[--Select--]				$0.00
13		[--Select--]	[--Select--]				$0.00
14		[--Select--]	[--Select--]				$0.00
15		[--Select--]	[--Select--]				$0.00

Total of Development Cost	$1,060,000 to $5,300,000
Total of Operational Cost	$1,165,000 to $8,485,000
Total Itemization of Costs:	$2,225,000 to $13,785,000

ADOA-ASET - Arizona Strategic Enterprise Technology
Project Investment Justification - Financials

Project ID:	To Be Provided by ADOA-ASET	Date Accepted:	To be Provided by ADOA-ASET

Project Information

Agency Name	Project Name	Date Submitted
Arizona Department of Revenue	Private Fraud Prevention Investigation Services	10/27/15

PIJ Development & Operational Cost Summary

Description	Type	Year 1	Year 2	Year 3	Year 4	Year 5	Extended Cost
Professional & Outside Services	Development						$0.00
	Operational	$250,000.00					$250,000.00
Hardware	Development						$0.00
	Operational						$0.00
Software	Development						$0.00
	Operational						$0.00
Communications	Development						$0.00
	Operational						$0.00
Facilities	Development						$0.00
	Operational						$0.00
Licensing & Maintenance Fees	Development						$0.00
	Operational						$0.00
Other	Development	$1,060,000 to $5,300,000					$1,060,000 to $5,300,000
	Operational	$0.00	$228,750 to $2,058,750	$228,750 to $2,058,750	$228,750 to $2,058,750	$228,750 to $2,058,750	$915,000 to $8,235,000
Development Cost:		$1,060,000 to $5,300,000	$0.00	$0.00	$0.00	$0.00	$1,060,000 to $5,300,000
Operational Cost:		$250,000.00	$228,750 to $2,058,750	$228,750 to $2,058,750	$228,750 to $2,058,750	$228,750 to $2,058,750	$1,165,000 to $8,485,000
Total Cost:							$2,225,000 to $13,785,000

Project Funding (add sources as appropriate)

Funding Source Category	Fund Name	Development Budget ($)		Operational Budget ($)		Total ($)
		Currently Available	New Request	Currently Available	New Request	
General Funds	Private Fraud Prevention Investigation Service	$2,900,000.00		$250,000.00	$915,000 to $8,235,000	$4,065,000 to $11,385,000
Federal Funds						$0.00
Other Appropriated Funds						$0.00
Other Non-Appropriated Funds						$0.00
Total Funding		$2,900,000.00	$0.00	$250,000.00	$915,000 to $8,235,000	$4,065,000 to $11,385,000