OFFICE OF THE
ARIZONA STATE TREASURER

KIMBERLY YEE
TREASURER

Request for Information

INVESMENT ACCOUNTING, PERFORMANCE REPORTING AND TRANSFER AGENCY SERVICES

1. INTRODUCTION

The Arizona State Treasurer Office (ASTO) hereby issues a Request for Information (RFI) from qualified vendors on the following scope of services. Vendors can choose to provide information on all or any of the services listed below.

- Investment Accounting
- Transfer agency
- Performance measurement and analytics

The purpose of this Request for Information (RFI) is to solicit information to assist the ASTO as it prepares to go out to competitive bid later this year or early next year for these services as part of a Master Custody contract.

This RFI is for planning purposes and should not be construed as a competitive solicitation nor should it be construed as an obligation on ASTO's part to enter into any contract or agreement. This RFI is not an invitation to pre-qualify potential applicants.

2. SCHEDULE OF EVENTS

RFI issued	October 6, 2023
Deadline for questions on RFI	October 26, 2023, 3:00 P.M. Local Arizona Time
Date for answers to questions on RFI	November 2, 2023, 10:00 A.M. Local Arizona Time
RFI deadline	November 9, 2023, 3:00 P.M. Local Arizona Time
Notification of firms selected to present	November 17, 2023, 3:00 P.M. Local Arizona Time
Presentations	December 4-13, 2023

Submittal Location:

Arizona State Treasurer's Office
1700 W. Washington St., Suite #102
Phoenix, AZ 85007

Electronic Submittals may be sent to: RFI@aztreasury.gov.

ASTO reserves the right to change dates and/or locations, as necessary.

3. OBTAINING A COPY OF THE RFI

All documents and information involving this RFI process are available from ASTO's internet site: https://www.aztreasury.gov/request-for-information

4. PREPARATION OF RESPONSE

4.1 All information shall be submitted in accordance with the instructions provided in this document. No submittal shall be altered, amended, or withdrawn after the specified due time and date.

4.2 It is the responsibility of all respondents to examine the entire RFI and seek clarification of any requirement that may not be clear and to check all responses for accuracy before submitting a response.

4.3 ASTO does not reimburse the cost of developing, presenting, or providing any response to this RFI. Responses submitted for consideration should be prepared simply and economically, providing adequate information in a straightforward and concise manner. The respondent is responsible for all costs incurred in responding to this RFI. All submittals in response to this RFI shall become the property of ASTO and become a matter of public record available for review pursuant to Arizona state law.

If a respondent believes that a specific section of its response is confidential, the respondent shall isolate the pages marked confidential in a specific and clearly labeled section of its response. The respondent shall include a written statement as to the basis for considering the marked pages confidential including the specific harm or prejudice disclosed. ASTO will review and make a determination.

5. INQUIRIES

All questions that arise relating to this RFI shall be directed in writing to RFI for Investment Accounting, Transfer Agency and Performance Reporting:

Jackie Harding
Deputy Treasurer Operations
Arizona State Treasurer's Office
1700 W. Washington St., Suite #102
Phoenix, AZ 85007

Or

RFI@aztreasury.gov

For written inquiries to be addressed, they must be received at the above address or email address by Thursday, October 26, 2023, at 3:00 P.M., Arizona Time. Inquiries received will then be answered in an addendum and published at https://www.aztreasury.gov/request-for-information.

6. SUBMISSION OF INFORMATION

Submittals must be in the actual possession of ASTO on or prior to the exact time and date indicated in the Schedule of Events.

Submittals must be submitted in a sealed envelope and the following information should be noted on the outside of the envelope:

Respondent's Name
Respondent's Address
Re: RFI: Investment Accounting, Performance Reporting and Transfer Agency Services.

Electronic Submittals may be sent to: RFI@aztreasury.gov

7. WITHDRAWAL OF SUBMITTAL

At any time prior to the RFI due date and time, a respondent (or designated representative) may withdraw the submittal by submitting a request in writing and signed by a duly authorized representative. Facsimiles, telegraph, or email withdrawals shall not be considered.

8. INFORMATION TO PROVIDE

OFFICE OF THE
ARIZONA STATE TREASURER

KIMBERLY YEE
TREASURER

8.1. The State of Arizona Treasurer's Office is entrusted with a variety of funds for safe-keeping and investing. Depending on the source of funds, they can be invested in overnight cash investments to long-only equities for endowment assets. As of June 30, 2023, total assets under management (AUM) were $31.1 billion.

The Treasurer's Office segregates the $31.1 billion-dollar investment program into four major participant types:

- Approximately $17.4 billion is considered State Agency Funds which are managed in nine (9) different fixed income pools, seven of those fixed income pools are managed by internal staff and two by one external manager. These pools are managed like bond mutual funds and have approximately 775 accounts.
- Approximately $5.9 billion is Local Government Investment Pools (LGIP). The LGIP consists of four investment pools and two are managed with a constant $1 Net Asset Value with a weighted average maturity of under 90 days and two with a floating NAV. 100% of the funds are managed by internal staff, and the funds have approximately 564 accounts.
- Approximately $7.8 billion is our Permanent Land Endowment Trust Fund (PLETF). The PLETF is 100% managed by internal staff on a total return basis with approximately 40% in two fixed income funds, and 60% are in three passive equity funds. The PLETF has 13 participants.
- Approximately $70 million is invested in the Arizona Endowment Trust Fund (AETF), also managed internally on a total return basis with 40% in fixed income and 60% in passive equity funds. The AETF has 4 participants.

8.2. RFIs should address the questions listed below. Vendors can respond to all three, or individually, the requests for information based upon the services offered by a vendor. Custodial banks may respond to the RFI but must identify the sub-contractor used to provide the services if not provided by the custodial bank directly.

Investment Accounting:

A. Provide a complete description of your investment accounting system.
B. Does your system have demonstrated integration with the following accounting platforms and trading systems: Bloomberg Aim; CGI Advantage, Infor?
C. What custodial banks does your system have experience in integrating with?
D. What basis of accounting do you use: trade date, settlement date?

E. What basis of accounting do you use for your general ledger cash or accrual?
F. How are you linked to custodial banks for settlement purposes?
G. Describe how you record interest received separately from interest accrued per security.
H. Provide a detailed listing of fixed income instruments supported by your accounting platform. Note: "Structured Notes" and "Mortgage Securities" are broad categories. Include a complete listing of those items supported and those that are not supported.
I. If an investment gets reclassified from one asset class to another, how does your system properly account for principal, premium/discount and interest allocated?
J. How are payoffs, paydowns and pay ups recorded?
K. Describe what reports are available from your system.
L. What pricing feeds do you use to value securities?
M. Are you able to provide an electronic file of daily purchases and maturities of securities including accounting for purchased interest, any premium or discount, the amortization of premium and discount, income (interest) received, income accrued, paydowns, pay-ups, amortization of interest and sort the information by pre-set asset classes?

Performance Reporting:

A. Describe the performance evaluation services you presently offer, including attribution analysis reports. What analytic platform supports this process?
B. Describe the methodology used to calculate performance measurement.
C. Provide a detailed listing of fixed income instruments supported by your analytic platform. Note: "Structured Notes" and "Mortgage Securities" are broad categories. Include a complete listing of those items supported and those that are not supported.
D. Do you adjust market values used in performance calculations for accruals?
E. What are the sources of your performance measurement and manager analytic information?
F. List all market indices available.
G. How often and how soon after the month-end are performance measurement reports available?
H. What pricing feeds do you use to value securities? How frequently are reports which are available within your system updated? i.e., real time, hourly, daily?
I. Are there capabilities for ad hoc reports to be created within the system?

Transfer Agency:

A. Provide a complete description of your transfer agency system.

B. Do you provide a web-based portal for clients to make transactions? Describe the security controls. Is there a "View Only" capability for users of the web-based portal?
C. Describe the process of entitling new users to the web-based system.
D. Provide examples of daily deposit/withdrawal transaction reports and daily account balance reports.
E. How soon after the end of the month are participant statements made available? How are they distributed?
F. What options do clients have to view/receive their statements?
G. What is the length of time that statements can be stored in the system?
H. Can prior statements be loaded into the system?
I. How long does it take to open a new account?
J. What information can be displayed on statements?
K. Can average balances for a specified period be provided?
L. Can client accounts be rolled up into a control group with the same reporting capabilities as an individual account?

9. STANDARD REQUEST FOR PROPOSAL (RFP) INFORMATION

Note: All the information below is in language that is part of a standard RFP and is not required to be filled out for this RFI. It is provided here so those responding to the RFI are aware of this requirement for State of Arizona RFPs and can provide comments on the ability to meet these AZRAMP requirements, or if the vendor is already FedRAMP certified.

WARRANTIES AND REQUIREMENTS RELATED TO ARIZONA INFORMATION TECHNOLOGY STATEWIDE POLICIES, STANDARDS, AND PROCEDURES

Security Standards

Security of the State's systems and data are of **utmost** importance to the State. In order to assure security from a personnel and operations perspective, Contractor shall comply with all requirements, in their entirety, as described in the statewide enterprise architecture; statewide Information Technology security policies, standards, and procedures; and any applicable agency-specific Information Technology security policies, standards, and procedures.

The Contractor shall follow the correct, current version of these policies, standards, and procedures. The current website for some of these policies, standards, and procedures is: Information Technology Policies, Standards and Procedures. Note that this link is provided for convenience only.

For security reasons, some state facilities require non-state personnel to have escorts. If required by the state facility, Contractor personnel shall only be allowed inside of a State facility if accompanied by an escort designated by the State. This is applicable in Correctional facilities, Public Safety facilities, State Lottery, and other facilities as designated by the State.

Prerequisite Assessment of Arizona Baseline Infrastructure Security Controls

To be susceptible for award, Offerors are required to complete and pass the Arizona Baseline Infrastructure Security Controls Prerequisite Assessment provided below and submit as separate attachment as part of the Offer.

Arizona Department of Homeland Security (AZDOHS) Cyber Command has established a NIST 800-53 revision 4 based process to assess risk associated with storing, processing, and transmitting State of Arizona Data with Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) vendors.

The State Data Classification Policy (8110) and a Confidentiality, Integrity, Availability (CIA) model are used to determine which level of assessment to administer for the vendor's Infrastructure / IaaS. A Microsoft Excel spreadsheet is currently used for each level of assessment.

The solicitation requires the Offeror to complete the Arizona Baseline Infrastructure Security Controls prerequisite assessment spreadsheet, which can be found at:

- https://azdohs.gov/file/4357
- Contractor is required to provide any requested documentation to include System Security Plan (SSP), policies, and procedures supporting the review of the assessment.

AZDOHS Cyber Command will evaluate, and rank submitted Arizona Baseline Infrastructure Security Controls for completeness, attention to detail, and understanding of NIST security controls and framework. AZDOHS Cyber Command will forward assessment results and recommendations to the Procurement Officer. Results of these IT security control reviews are for internal use only and will not be shared with responding bidders but may impact the Offeror's susceptibility for award.

All Offerors must complete the assessment above, and complete with their Offers as a separate attachment. This task is a mandatory requirement for an Offeror to be considered for award.

*NOTE: If the contractor will be receiving data solely from a third party and NOT any State of Arizona agency or entity, the contractor will not need to undergo an AZRAMP assessment. The State will assume that an AZRAMP assessment is required until the bidder proves otherwise.
In the State's sole discretion, the State may also accept current FedRAMP and StateRAMP certifications as evidence that the Contractor has met the State's risk assessment requirements. Other forms of Cybersecurity Frameworks (CSF), Trust Documents, Self-Attestations, including, but not limited to, ISO/IEC, SOC 2 & 3, PCI, or HIPAA reports of compliance, may be reviewed as part of the State's risk assessment, but are not exclusive or conclusive evidence that the Contractor has met the State's risk assessment requirements.

Additional Security Requirements

The State reserves the right to conduct risk assessments, vulnerability assessments, black-box penetration tests or hire a third party to conduct risk assessments, vulnerability assessments, and black-box penetration tests of the Contractor's environment. The contractor will be alerted in advance and arrangements made for an agreeable time. The contractor shall respond to all flaws deemed serious by the State when discovered by providing an acceptable timeframe to resolve the issue and/or implement a compensating control(s).

Upon request, Contractor shall submit copies of system logs from Contractor's environment to the State of AZ security team in the format requested to be added to the State SIEM (Security Information Event Monitor) or IDS (Intrusion Detection System).

Contractor shall comply with all applicable State and Federal laws and regulations, including, but not limited to, the following (please note that the links are provided for convenience only and may change):

- State of Arizona statewide policies, standards, and procedures: https://azdohs.gov/information-technology-it-policies-standards-and-procedures;
- Federal Information Security Modernization Act of 2014 (FISMA): https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma;

- OMB Circular A-130: https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource;
- National Cyber Strategy of the United States of America: https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure;
- Health Insurance Portability and Accountability Act (HIPAA) including Business Associate Agreement/ Health Information Technology for Economic and Clinical Health Act (HITECH): https://www.hhs.gov/hipaa/index.html;
- Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information (IRS Publication 1075): https://www.irs.gov/pub/irs-pdf/p1075.pdf;
- Criminal Justice Information Services Security Policy (CJIS): https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center;
- Centers for Medicare & Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E): https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2-MARS-E-v2-0-Minimum-Acceptable-Risk-Standards-for-Exchanges-11102015.pdf;
- A.R.S. Title 41, Chapter 41. Arizona Department of Homeland Security;
- A.R.S. §18-104 - Arizona Department of Administration, Arizona Strategic Enterprise Technology (ADOA-ASET), Powers and duties of the agency: https://www.azleg.gov/arsDetail/?title=18;
- A.R.S. §18-105 - Statewide Information Security and Privacy Office (SISPO): https://www.azleg.gov/viewdocument/?docName=http%3A//www.azleg.gov/ars/18/00105.htm;
- A.R.S. §18-551 - Definitions Information Security Including PII: https://www.azleg.gov/ars/18/00551.htm;
- A.R.S. §18-552 - Notification of security system breaches; requirements; enforcement; civil penalty; preemption; exceptions: https://www.azleg.gov/ars/18/00552.htm;
- Arizona Executive Order 2008-10 – Mitigating Cyber Security Threats: https://aset.az.gov/node/192;
- SIPC Memorandum of Understanding (MOU): https://www.sipc.org/about-sipc/;

- State Environmental policies: https://azdeq.gov/LawsAndRules;
- Family Education Rights Privacy Act (FERPA): https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn;
- Driver's Privacy Protection Act (DPPA): https://azdot.gov/motor-vehicles/driver-services/driver-license-information/motor-vehicle-records;
- Incident Response Reporting program and system: https://aset.az.gov/sites/default/files/P8240%20Incident%20Response%20Planning_Sept2018_0.pdf;
- Privacy Incident Reporting policy and standards: https://aset.az.gov/sites/default/files/STANDARD%208240%20INCIDENT%20RESPONSE%20PLANNING.pdf;
- State of Arizona Library, Archives and Public Records, Records Management Division, General Retention Schedules https://azlibrary.gov/arm/policies; and
- Payment Card Industry (PCI) Security Standards including but not limited to Supplemental Documents, Information Supplements and Validation Requirements: https://www.pcisecuritystandards.org.

DATA AND INFORMATION HANDLING:

This section applies to the extent the Work includes handling of any (1) State's proprietary and sensitive data or (2) confidential or access-restricted information obtained from State or from others at State's behest.

Data Protection and Confidentiality of Information. Contractor warrants that it will establish and maintain procedures and controls acceptable to State for ensuring that State's proprietary and sensitive data is protected from unauthorized access and information obtained from State or others in performance of its contractual duties is not mishandled, misused, or inappropriately released or disclosed. For purposes of this paragraph, all data created by Contractor in any way related to the Contract, provided to Contractor by State, or prepared by others for State are proprietary to State, and all information by those same avenues is State's confidential information. To comply with the foregoing warrant:

1. Contractor shall: (a) notify State immediately of any unauthorized access or inappropriate disclosures, whether stemming from an external security breach, internal breach, system failure, or procedural lapse; (b) cooperate with State to identify the source or cause and respond to each unauthorized access or inappropriate disclosure; and (c) notify State promptly of any security threat that could result in unauthorized access or inappropriate

disclosures; and

2. Contractor shall not: (a) release any such data or allow it to be released or divulge any such information to anyone other than its employees or officers as needed for each person's individual performance of his or her duties under the Contract, unless State has agreed otherwise in advance and in writing; or (b) respond to any requests it receives from a third party for such data or information, and instead route all such requests to State's designated representative.

Personally Identifiable Information. Without limiting the generality of this paragraph, Contractor warrants that it will protect any personally identifiable information ("PII") belonging to State's employees or other contractors or members of the general public that it receives from State or otherwise acquires in its performance under the Contract. For purposes of this paragraph:

1. PII has the meaning given in the [federal] Office of Management and Budget (OMB) Memorandum M-17-12 Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017; and

2. "Protect" means taking measures to safeguard personally identifiable information and prevent its breach that are functionally equivalent to those called for in that OMB memorandum and elaborated on in the [federal] General Services Administration (GSA) Directive CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information.

   NOTE (1): For convenience of reference only, the OMB memorandum is available at: https://dpcld.defense.gov/Privacy/Authorities-and-Guidance/

   NOTE (2): For convenience of reference only, the GSA directive is available at:

   https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-(pii)-

   Protected Health Information. Contractor warrants that, to the extent performance under Contract involves individually identifiable health information (referred to hereinafter as protected health information ("PHI") and electronic PHI ("ePHI") as defined in the Privacy Rule referred to below), it:

   a. is familiar with and will comply with the applicable aspects of the following collective regulatory requirements regarding patient information privacy protection: (a) the

"Privacy Rule" in CFR 45 Part 160 and Part 164 pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996; (b) Arizona laws, rules, and regulations applicable to PHI/ePHI that are not preempted by CFR45-160(B) or the Employee Retirement Income Security Act of 1974 ("ERISA") as amended; and (c) State's current and published PHI/ePHI privacy and security policies and procedures;

b. will cooperate with State in the course of performing under the Contract so that both State and Contractor stay in compliance with the requirements in (1) above; and

c. will sign any documents that are reasonably necessary to keep both State and Contractor in compliance with the requirements in (1) above, in particular "Business Associate Agreements" in accordance with the Privacy Rule.

NOTE: For convenience of reference only, the Privacy Rule is available at:
http://www.hhs.gov/hipaa/for-professionals/privacy/index.html

INFORMATION TECHNOLOGY WORK: this section applies to any Invitation for Bids, Request for Proposals, or Request for Quotations for "Information Technology," as defined In A.R.S. §18-101 -6 "…all computerized and auxiliary automated information processing, telecommunications and related technology, including hardware, software, vendor support and related services, equipment and projects," if and to the extent that the Work is or includes Information Technology.

Background Checks. Each Contractor's personnel who is an applicant for an information technology position must undergo the security clearance and background check procedure, which includes fingerprinting, as required by A.R.S. §41-710. Contractor shall obtain and pay for the security clearance and background check. Contractor personnel who will have administrator privileges on a State network must additionally provide identity and address verification and undergo State-specified training for unescorted access, confidentiality, privacy, and data security.

Information Access

1. SYSTEM MEASURES. The Contractor shall employ appropriate system management and maintenance, fraud prevention and detection, and encryption application and tools to any systems or networks containing or transmitting State's proprietary data or confidential information.

2. INDIVIDUAL MEASURES. Contractor personnel shall comply with applicable State

policies and procedures regarding data access, privacy, and security, including prohibitions on remote access and obtaining and maintaining access identifications (IDs) and passwords. The contractor is responsible to the State for ensuring that any State access IDs and passwords are used only by the person to whom they were issued. Contractor shall ensure that personnel are only provided the minimum only such level of access necessary to perform his or duties. The contractor shall on request, provide a current register of the access IDs and passwords and corresponding access levels currently assigned to its personnel.

3. ACCESS CONTROL. Contractor is responsible to State for ensuring that hardware, software, data, information, and that has been provided by State or belongs to or is in the custody of State and is accessed or accessible by Contractor personnel is only used in connection with carrying out the Work and is never commercially exploited in any manner whatsoever not expressly permitted under the Contract. State may restrict access of Contractor personnel, or instruct Contractor to restrict their access, if in its determination the requirements of this subparagraph are not being met.

Pass-Through Indemnity

1. INDEMNITY FROM THIRD PARTY. For computer hardware or software included in the Work as discrete units that were manufactured or developed solely by a third party, Contractor may satisfy its indemnification obligations under the Contract by, to the extent permissible by law, passing through to State such indemnity as it receives from the third-party source (each a "Pass-Through Indemnity") and cooperating with State in enforcing that indemnity. If the third party fails to honor its Pass-Through Indemnity, or if a Pass-Through Indemnity is insufficient to indemnify State Indemnitees to the extent and degree, Contractor is required to do by the Uniform Terms and Conditions, then Contractor shall indemnify, defend, and hold harmless State Indemnitees to the extent the Pass-Through Indemnity does not.

2. NOTIFY OF CLAIMS. State shall notify Contractor promptly of any claim to which a Pass-Through Indemnity might apply. Contractor, with reasonable consultation from State, shall control of the defense of any action on any claim to which a Pass-Through Indemnity applies, including negotiations for settlement or compromise, provided that:
    a. State reserves the right to elect to participate in the action at its own expense;
    b. State reserves the right to approve or reject any settlement or compromise on reasonable grounds and if done so timely; and
    c. State shall in any case cooperate in the defense and any related settlement negotiations.

Systems and Controls: In consideration for State having agreed to permit Pass-Through

Indemnities in lieu of direct indemnity, Contractor agrees to establish and keep in place systems and controls appropriate to ensure that State funds under this Contract are not knowingly used for the acquisition, operation, or maintenance of Materials or Services in violation of intellectual property laws or a third party's intellectual property rights.

Redress of Infringement

1. REPLACE, LICENSE, OR MODIFY. If Contractor becomes aware that any Materials or Services infringe, or are likely to be infringing, on any third party's intellectual property rights, then Contractor shall, at its sole cost and expense and in consultation with State, either:
   a. replace any infringing items with non-infringing ones;
   b. obtain for State the right to continue using the infringing items; or
   c. modify the infringing items so that they become non-infringing, so long as they continue to function as specified following the modification.

2. CANCELLATION OPTION. In every case listed above, if none of those options can reasonably be accomplished, or if the continued use of the infringing items is impracticable, State may cancel the relevant Order or terminate the Contract, and Contractor shall take back the infringing items. If State does cancel the Order or terminate the Contract, Contractor shall refund to State:
   a. for any software created for State under the Contract, the amount State paid to Contactor for creating it;
   b. for all other Materials, the net book value of the product provided according to generally accepted accounting principles; and
   c. for Services, the amount paid by State or an amount equal to 12 (twelve) months of charges, whichever is less.

3. EXCEPTIONS. Contractor will not be liable for any claim of infringement based solely on any of the following by a State Indemnitee:
   a. modification or use of Materials other than as contemplated by the Contract or expressly authorized or proposed by a Contractor Indemnitor;
   b. operation of Materials with any operating software other than that supplied by Contractor or authorized or proposed by a Contractor Indemnitor; or
   c. combination or use with other products in a manner not contemplated by the Contract or expressly authorized or proposed by a Contractor Indemnitor.

First Party Liability Limitation

1. LIMIT. Subject to the provisos that follow below and unless stated otherwise in the Special

Terms and Conditions, State's, and Contractor's respective first party liability arising from or related to the Contract is limited to the greater of $1,000,000 (one million dollars) or 3 (three) times the purchase price of the specific Materials or Services giving rise to the claim.

2. PROVISOS. This paragraph limits liability for first party direct, indirect, incidental, special, punitive, and consequential damages relating to the Work regardless of the legal theory under which the liability is asserted. This paragraph does not limit liability arising from any:
   a. Indemnified Claim against which Contractor has indemnified State Indemnitees
   b. claim against which Contractor has indemnified State Indemnitees; or
   c. provision of the Contract calling for liquidated damages or specifying amounts or percentages as being at-risk or subject to deduction for performance deficiencies.

3. PURCHASE PRICE DETERMINATION. If the Contract is for a single-agency and a single Order (or if no Order applies), then "purchase price" in Subparagraph 14.7.1 above means the aggregate Contract price current at the time of Contract expiration or earlier termination, including all Contract Amendments having an effect on the aggregate price through that date. In all other cases, "purchase price" above means the total price of the Order for the specific equipment, software, or services giving rise to the claim, and therefore a separate limit will apply to each Order.

4. NO EFFECT ON INSURANCE. This paragraph does not modify the required coverage limits, terms, and conditions of, or any insured's ability to claim against any insurance that Contractor is required by the Contract to provide, and Contractor shall obtain express endorsements that it does not.

<u>Information Technology Warranty</u>

1. SPECIFIED DESIGN. Where the Scope of Work for information technology, Work provides a detailed design specification or sets out specific performance requirements, Contractor warrants that the Work will provide all functionality material to the intended use stated in the Contract, provided that, the foregoing warranty does not extend to any portions of the Materials that are:
   a. modified or altered by anyone not authorized by Contractor to do so;
   b. maintained in a way inconsistent to any applicable manufacturer recommendations; or
   c. operated in a manner not within its intended use or environment.

2. COTS SOFTWARE. With respect to Materials provided under the Contract that are commercial-off-the-shelf (COTS) software, Contractor warrants that:
   a. to the extent possible, it will test the software before delivery using commercially available virus detection software conforming to current industry standards;

b. the COTS software will, to the best of its knowledge, at the time of delivery be free of viruses, backdoors, worms, spyware, malware, and other malicious code that could hamper performance, collect unlawfully any personally identifiable information, or prevent products from performing as required by the Contract; and
c. it will provide a new or clean install of any COTS software that State has reason to believe contains harmful code.

3. PAYMENT HAS NO EFFECT. The warranties in this paragraph are not affected by State's inspection, testing, or payment.

Specific Remedies. Unless expressly stated otherwise elsewhere in the Contract, State's remedy for breach of warranty includes, at State's discretion, re-performance, repair, replacement, or refund of any amounts paid by State for the nonconforming Work, plus (in every case) Contractor's payment of State's additional, documented, and reasonable costs to procure materials or services equivalent in function, capability, and performance that was first called for. For clarification of intent, the foregoing obligations are limited by the limitation of liability. If none of the forgoing options can reasonably be affected, or if the use of the materials by State is made impractical by the nonconformance, then State may seek any remedy available to it under law.

Section 508 Compliance. Unless specifically authorized in the Contract, any electronic or information technology offered to the State of Arizona under this Contract shall comply with A.R.S. §18-131 and §18-132 and Section 508 of the Rehabilitation Act of 1973, which requires that employees and members of the public shall have access to and use of information technology that is comparable to the access and use by employees and members of the public who are not individuals with disabilities.

Cloud Applications. The following are required for Contractor of any cloud solution that hosts State data outside of the State's network or transmits and/or receives State data.

1. Submit a completed Arizona Baseline Infrastructure Security Controls assessment spreadsheet as found at: https://aset.az.gov/resources/policies-standards-and-procedures, and mitigate or install compensating controls for any issues of concern identified by State. Contractor is required to provide any requested documentation supporting the review of the assessment. The assessment shall be re-validated on a minimum annual basis.

2. The State reserves the right to conduct penetration tests or hire a third party to conduct penetration tests of the Contractor's application. The contractor will be alerted in advance and arrangements made for an agreeable time. The contractor shall respond to all serious flaws discovered by providing an acceptable timeframe to resolve the issue and/or

implement a compensating control.

3. Contractors must submit a copy of system logs from the cloud system to the State of Arizona security team on a regular basis to be added to the State SIEM (Security Information Event Monitor) or IDS (Intrusion Detection System).

4. The contractor must employ a government-rated cloud compartment to better protect sensitive or regulated State data.

10. RESPONDENT INFORMATION AND AUTHORIZATION

Respondent certifies they have read and fully understands this RFI.

Submitted by:

Signature: _____

Typed Name: _____

Title: _____

Date: _____