



IE – HHS – BI Project System Security Control Assessment (SCA) V5

R E Q U E S T F O R Q U O T A T I O N

State Term Schedule

Table of Contents

| | |
|--|-------|
| INTRODUCTION AND BACKGROUND..... | 3 |
| PURPOSE OF THE REQUEST FOR QUOTATION | 3 |
| BACKGROUND | 3 |
| STATEMENT OF WORK (SOW)..... | 3-10 |
| ADMINISTRATIVE | 11 |
| PROPOSAL INQUIRIES | 11 |
| DUE DATES | 12 |
| SCHEDULE OF EVENTS..... | 12 |
| EVALUATION FACTORS FOR AWARD | 12-13 |
| EVALUATION | 12-13 |
| TERM AND CONTRACT | 13 |
| STATUS REPORTING..... | 13 |
| NON-DISCLOSURE AGREEMENT | 13 |
| GUIDELINES FOR QUOTATION PREPARATION..... | 13-16 |
| QUOTATION SUBMITTAL | 13 |
| PROPRIETARY INFORMATION | 14 |
| WAIVER OF DEFECTS..... | 14 |
| REJECTION OF QUOTATIONS..... | 15 |
| EVALUATION OF QUOTATIONS | 15-16 |
| ATTACHMENT ONE | 17-19 |

INTRODUCTION AND BACKGROUND

PURPOSE OF THE REQUEST FOR QUOTATION

Please consider this as the State of Ohio, Department of Administration, and Office of Information Technology (OIT) Request for Quotation for the following project:

IE HHS BI Project System Security Control Assessment (SCA) V5

The State of Ohio is requesting no more than three (3) resumes per vendor and quotation for a Business Intelligence Project System Security Control Assessment (SCA) V5. The role is needed as of **August 1, 2013**.

BACKGROUND

The State of Ohio Office of Medical Assistance (OMA) and Department of Administrative Services (DAS) awarded a contract to Accenture in February of 2013 to build an enterprise system to provide Medicaid Integrated Eligibility System. In support of this system, OMA and DAS contracted with Truven Health Analytics to build a Business Intelligence System.

Operation of these systems is dependent on approval by the Centers for Medicare & Medicaid Services (CMS) of the system. This requires we obtain a Systems Control Assessment (SCA).

Statement of Work (SOW)

The vendor will supply a Systems Control Assessment for the Integrated Eligibility and Business Intelligence Systems. Both systems are defined with a Security Control Baseline of NIST 800-53 R3 Moderate. The design includes:

| | Integrated Eligibility | Business Intelligence |
|--------------|---|-----------------------|
| Applications | SOA-based Java JEE applications and portals, based primarily on the following technology platforms: <ul style="list-style-type: none">· Oracle Fusion Middleware· Oracle Policy Automation· Oracle Identity & Access Management· Adobe, Informatica, and | ERWIN and Teradata |

| | | |
|------------|---|--|
| | IBM Cognos BI software platforms | |
| Servers | Physical Exadata Devices – 3 Physical Exalogic Devices – 3 Rackmount Servers – approx. 30 Virtual Servers – Between 100-150 (final counts TBD) | 20 |
| Users | Up to 1435 internal users. Citizen users based on state ACA legislation. | 340 and 640 users in total, with a maximum of 128 concurrent users |
| Managed by | Accenture | Truven |

Specifically, the Assessment must:

1. Adhere to NIST Special publications 800-53 and 800-37. (Note: NIST 800-53A not in scope. The State of Ohio uses SANS Consensus Audit Guidelines (CAG 2.3 or the current version) for its implementation and compliance guidance of the NIST 800.53 framework. A copy of CAG 2.3 can be provided upon request after award.)
2. Adhere to State of Ohio laws and policies. State of Ohio policies can be found at: <http://privacy.ohio.gov/OhioPolicies.aspx>
3. A minimum of 170 required security controls and 93 required control enhancements are anticipated to be evaluated.
4. Controls categorized as Technical, Operational, and Management. These controls span 18 Control Families (Ex. Access Control – AC, Contingency Planning – CP, etc.).
5. Disaster Recovery sites are part of the scope of this project for both environments. It is anticipated the sites may not be ready in time for this assessment. Review of completed documentation and Plan of Action and Milestones (POAM) may be used if the sites are not ready.
6. **The final determination of the inclusion of Internal Revenue Data (IRS) data in the Integrated Eligibility system is not expected but this decision has not been finalized.** Therefore, preparation of a Safeguards Procedures Report (SPR) has yet to be determined. Please include a price and contingency plans if an SPR is required.
7. Implementation responsibilities span all project work streams. Communication and coordination with the work stream Leads will be necessary. Security control implementation details are contained in the SSP which will be provided after award.
8. Judgmental sampling is acceptable and anticipated where appropriate. Please explain when and where you anticipate using this technique.
9. This SCA is based on assessment of controls. No penetration testing is expected.

It is anticipated that both systems be evaluated at the same time but due to schedule and other unforeseen project delays, separate assessment may be required. Any quote submitted must allow for this contingency.

| Deliverable # | Deliverable Name | Deliverable Description | Cost of Each Deliverable | Deliverable Timeline |
|---------------|-------------------------------------|--|--------------------------|----------------------|
| 1 | Assessment Preparation | Develop, review, and approve a plan to assess the security controls. (See Appendix A for details) | | |
| 2 | Security Control Assessment | Access the security controls in accordance with the assessment procedures defined in the security assessment plan. (See Appendix A for details) | | |
| 3 | Security Assessment Report | Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment. (See Appendix A for details) | | |
| 4 | Remediation Recommendations Actions | Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate. (See Appendix A for details) | | |

APPENDIX A

TASK 1: Develop, review, and approve a plan to assess the security controls. This should include a timeline for the overall SCA approach covering assessment through remediation.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions). Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with

reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments. The security assessment plan is reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security objectives of the organization, employs state-of-the-practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, and is cost effective with regard to the resources allocated for the assessment. The purpose of the security assessment plan approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment. An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining security control effectiveness. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization obtains a security assessment plan from the provider.

Organizations consider both the technical expertise and level of independence required in selecting security control assessors. Organizations also ensure that security control assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security controls. The authorizing official or designated representative determines the required level of independence for security control assessors based on the results of the security categorization process for the information system and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a risk-based decision on whether to place the information system into operation or continue its operation. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the security control assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official consults with the Office of the Inspector General, the senior information security officer, and the chief information officer to discuss the implications of any decisions on assessor independence in the types of special circumstances described above. This discussion may occur prior to each security assessment or only once if an organization is establishing an organizational policy and approach for specific special circumstances that will be applied to all information systems meeting the specific special circumstance

criteria. Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors.

SECURITY CONTROL ASSESSMENT

TASK 2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system. These types of assessments are referred to as developmental testing and evaluation and are intended to validate that the required security controls are implemented correctly and consistent with the established information security architecture. Developmental testing and evaluation activities include, for example, design and code reviews, application scanning, and regression testing. Security weaknesses and deficiencies identified early in the system development life cycle can be resolved more quickly and in a much more cost-effective manner before proceeding to subsequent phases in the life cycle. The objective is to identify the information security architecture and security controls up front and to ensure that the system design and testing validate the implementation of these controls.

The information system owner relies on the technical expertise and judgment of assessors to: (i) assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings are an unbiased, factual reporting of the weaknesses and deficiencies discovered during the security control assessment.

The organization ensures that assessors have access to: (i) the information system and environment of operation where the security controls are employed; and (ii) the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls. In addition, assessors have the required degree of independence as determined by the authorizing official. Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, facilitates reuse of assessment results when reauthorization is required. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization ensures that assessors have access to the information system/environment of operation where the controls are employed as well as appropriate information needed to carry out the assessment. The organization also

obtains any information related to existing assessments that may have been conducted by the external provider and reuses such assessment information whenever possible in accordance with the reuse criteria established by the organization. Descriptive information about the information system is typically documented in the system identification section of the security plan or included by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation are identified as well. In order to make the risk management process as timely and cost-effective as possible, the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended. For example, a recent audit of an information system may have produced information about the effectiveness of selected security controls. Another opportunity to reuse previous assessment results comes from programs that test and evaluate the security features of commercial information technology products. Additionally, if prior assessment results from the system developer are available, the security control assessor, under appropriate circumstances, may incorporate those results into the assessment. And finally, assessment results are reused to support reciprocity where possible.

SECURITY ASSESSMENT REPORT

TASK 3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner or Common Control Provider; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational and/or federal policies. The reporting format is also appropriate for the type of security control assessment conducted (e.g., developmental testing and evaluation, self-assessments, independent verification and validation, independent assessments supporting the security authorization process or subsequent reauthorizations, assessments during continuous monitoring, assessments subsequent to remediation actions, independent audits/evaluations).

Security control assessment results obtained during system development are brought forward in an interim report and included in the final security assessment report. This supports the concept that the security assessment report is an evolving document that includes assessment results from all relevant phases of the

system development life cycle including the results generated during continuous monitoring. Organizations may choose to develop an executive summary from the detailed findings that are generated during a security control assessment. An executive summary provides an authorizing official with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.

REMEDATION RECCOMENDATION ACTIONS

TASK 4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Primary Responsibility: Information System Owner or Common Control Provider; Security Control Assessor.

Supporting Roles: Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer; Information System Security

Engineer; Security Control Assessor.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The security assessment report provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system that could not reasonably be resolved during system development. The findings generated during the security control assessment facilitate a disciplined and structured approach to mitigating risks in accordance with organizational priorities. Information system owners and common control providers, in collaboration with selected organizational officials (e.g., information system security engineer, authorizing official designated representative, chief information officer, senior information security officer, information owner/steward), may decide that certain findings are inconsequential and present no significant risk to the organization. Alternatively, the organizational officials may decide that certain findings are in fact, significant, requiring immediate remediation actions. In all cases, organizations review assessor findings and determine the severity or seriousness of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation) and whether the findings are sufficiently significant to be worthy of further investigation or remediation. An updated assessment of risk (either formal or informal) based on the results of the findings produced during the security control assessment and any inputs from the risk executive (function), helps to determine the initial remediation actions and the prioritization of such actions. Senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions and business functions for the organization or correcting the deficiencies that pose the greatest degree of risk. If weaknesses or deficiencies in security controls are corrected, the remediated controls are reassessed for effectiveness. Security control reassessments determine the extent to which the remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Exercising caution not to

change the original assessment results, assessors update the security assessment report with the findings from the reassessment. The security plan is updated based on the findings of the security control assessment and any remediation actions taken. The updated security plan reflects the actual state of the security controls after the initial assessment and any modifications by the information system owner or common control provider in addressing recommendations for corrective actions. At the completion of the assessment, the security plan contains an accurate list and description of the security controls implemented (including compensating controls) and a list of residual vulnerabilities.

Organizations can prepare an optional addendum to the security assessment report that is transmitted to the authorizing official. The optional addendum provides information system owners and common control providers an opportunity to respond to the initial findings of assessors. The addendum may include, for example, information regarding initial remediation actions taken by information system owners or common control providers in response to assessor findings, or provide an owner's perspective on the findings (e.g., including additional explanatory material, rebutting certain findings, and correcting the record). The addendum to the security assessment report does not change or influence in any manner, the initial assessor findings provided in the original report. Information provided in the addendum is considered by authorizing officials in their risk-based authorization decisions. Organizations may choose to employ an issue resolution process to help determine the appropriate actions to take with regard to the security control weaknesses and deficiencies identified during the assessment. Issue resolution can help address vulnerabilities and associated risk, false positives, and other factors that may provide useful information to authorizing officials regarding the security state of the information system including the ongoing effectiveness of system-specific, hybrid, and common controls.

The issue resolution process can also help to ensure that only substantive items are identified and transferred to the [plan of actions and milestones. RECCOMENDATIONS AND REMEDIATION DATES.](#)

Sourced from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf> CHAPTER 3. Testing process only.

REMINDER: This is to be complaint with NIST 800-53 R3 only. Not derived from 800-53A. (Note: NIST 800-53A not in scope. The State of Ohio uses SANS Consensus Audit Guidelines (CAG 2.3 or the current version) for its implementation and compliance guidance of the NIST 800.53 framework. This is outlined in State of Ohio Policy ITS-SEC-02 - Enterprise Security Controls Framework.)

ADMINISTRATIVE

PROPOSAL INQUIRIES

Vendors may make inquiries regarding this RFQ any time during the inquiry period listed on the RFQ cover sheet. The State may not respond to any improperly formatted inquiries. The State will try to respond to all inquiries within 24 hours, excluding weekends and State holidays. The State will not respond to any inquiries received after 8:00 am on the inquiry period end date. The State may extend the proposal due date.

To make an inquiry, vendors must use the process outlined below.

- Access the State Procurement Web site at <http://procure.ohio.gov/>.
- From the Navigation Bar on the left, select “Find It Fast”.
- Select “Doc/Bid/Schedule #” as the Type.
- Enter the RFQ number found on the first page of this RFQ (the RFQ number begins with “DAS”).
- Click the “Find It Fast” button.
- On the document information page, click the “Submit Inquiry” button.
- On the document inquiry page, complete the required “Personal Information” section by providing:
 - First and last name of the prospective vendor’s representative who is responsible for the inquiry;
 - Name of the prospective vendor;
 - Representative’s business phone number, and
 - Representative’s e-mail address.
- Type the inquiry in the space provided, including:
 - A reference to the relevant part of this RFQ;
 - The heading for the provision under question, and
 - The page number of the RFQ where the provision can be found.
 - Click the “Submit” button.

A vendor submitting an inquiry will receive an immediate acknowledgement that the State has received the inquiry as well as an e-mail acknowledging receipt. The vendor will not receive a personalized response to the question nor notification when the State has answered the question.

Vendors may view inquiries and responses on the State’s Procurement Web site by using the “Find It Fast” feature described above and by clicking the “View Q & A” button on the document information page.

All questions must be submitted by 8:00 am on July 12, 2012. Questions submitted after this time will not receive a response from the state.

DUE DATES

All quotations are due by 1:00 pm, EST, on July 17, 2013. Any quotation received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late quotations will not be evaluated for award.

SCHEDULE OF EVENTS

All times listed is Eastern Standard Time (EST).

| Event | Date |
|---|----------------------------------|
| 1. RFQ Distribution to Vendors | July 5, 2013 |
| 2. Questions from Vendors due | 8:00 a.m., July 12, 2013 |
| 3. Responses to Vendors due | 4:00 p.m., July 15, 2013 |
| 4. Proposal/Quotation Due Date | 1:00 p.m., July 17, 2013 |
| 5. Target Date for Review of Proposal/Quotation | July 17, 2013 – July 18, 2013 |
| 6. Interviews of Candidates, if needed | July 19, 2013 – July 22, 2013 |
| 7. Anticipated decision and selection of Vendor | July 24, 2013 |
| 8. Anticipated commencement date of work | On or after August 1, 2013 |

VALUATION FACTORS FOR AWARD

EVALUATION

The following will be considered in determining the vendor to be selected for this engagement,

according to a standardized scoring methodology:

- Relevant experience
- Relevant skill level
- Proposed contractor rate(s)

TERM AND CONTRACT

The contract will be through State Term Schedule (STS) contracts and must reflect or be lower than STS rates, and must use STS categories.

STATUS REPORTING

The contractor will provide weekly status reports to the State OIT. The contractor will be responsible for meeting all timelines designated by assigned Project manager. Payment for services will be based on deliverable completion subject to the State's approval of each deliverable. The State will review deliverables and provide feedback or approval for each deliverable within 5 business days of receipt of deliverable.

NON-DISCLOSURE AGREEMENT

Both candidate and company will be required to sign a non-disclosure agreement which prevents disclosure of any data obtained while on the engagement which can be used to personally identify any parties at any time either during or after the engagement.

GUIDELINES FOR QUOTATION PREPARATION

QUOTATION SUBMITTAL

Each Vendor must submit three (3) complete, sealed and signed copies of its quotation and each quotation must be clearly marked "IE HHS BI Project SCA V5" on the outside of its envelope along with Vendors name.

A single electronic copy of the complete quotation must also be submitted with the printed quotations. Electronic submissions should be on a CD, DVD or USB memory stick.

Each proposal must be organized in the same format as described below. Any material deviation from the format outlined below may result in a rejection of the non-conforming proposal. Each proposal must contain an identifiable tab sheet preceding each section of the proposal. Quote should be good for a minimum of 45 days.

- Cover Letter (include phone and e-mail contact)
- State Term Schedule Number
- STS Labor Category Code
- Vendor Information:
 - Vendor References (3 minimum) - form
 - Vendor Resume
 - Additional Vendor Information (optional) – vendor form
- Vendor Hourly Rate
- Cost of Deliverables
- Deliverable Timeline

- Conflict of Interest Statement
- Payment Address
- Proof of Insurance
- W-9 Form

The State will not be liable for any costs incurred by any offeror in responding to this RFQ, even if the State does not award a contract through this process. The State may decide not to award a contract at the State's discretion. The State may reject late quotations regardless of the cause for the delay. The State may also reject any quotation that it believes is not in its interest to accept and may decide not to do business with any of the Vendors responding to this RFQ.

Quotations MUST be submitted to the State's Procurement Representative:

Ms. Nychola Richardson, MAS1
30 East Broad Street, 39th Floor
Columbus, OH 43215

PROPRIETARY INFORMATION

All quotations and other material submitted will become the property of the State and may be returned only at the State's option. Proprietary information should not be included in a quotation or supporting materials because the State will have the right to use any materials or ideas submitted in any quotation without compensation to the Vendor. Additionally, all quotations will be open to the public after the contract has been awarded.

The State may reject any Proposal if the Vendor takes exception to the terms and conditions of this RFQ.

WAIVER OF DEFECTS

The State has the right to waive any defects in any quotation or in the submission process followed by a Vendor. But the State will only do so if it believes that is in the State's interest and will not cause any material unfairness to other Vendors.

REJECTION OF QUOTATIONS

The State may reject any quotation that is not in the required format, does not address all the requirements of this RFQ, or that the State believes is excessive in price or otherwise not in its interest to consider or to accept. The State will reject any Non-STS responses. In addition, the State may cancel this RFQ, reject all the quotations, and seek to do the work through a new RFQ or other means.

EVALUATION OF QUOTATIONS

Clarifications and Corrections

During the evaluation process, the State may request clarifications from any Vendor under active consideration. It also may give any Vendor the opportunity to correct defects in its quotation. But the State will allow corrections only if they do not result in an unfair advantage for the Vendor and it is in the State's best interest.

Requirements

This RFQ asks for responses and submissions from Vendors. While each criterion represents only a part of the total basis for a decision to award the contract to a Vendor, a failure by a Vendor to make a required submission or meet a requirement will normally result in a rejection of that Vendor's quotation. The value assigned to each criterion is only a value used to determine which quotation is the most advantageous to the State in relation to the other quotations that the State received. It is not a basis for determining the importance of meeting any requirement to participate in the quotation process.

The evaluation process may consist of up to three distinct phases:

1. The procurement representative's initial review of all quotations for defects;
2. The evaluation committee's evaluation of the quotations; and
3. Interviews (optional).

Initial Review

The procurement representative normally will reject any incomplete or incorrectly formatted quotation, though the procurement representative may elect to waive any defects or allow a Vendor to submit a correction. If a late quotation is rejected, the procurement representative will not open or evaluate the late quotations. The procurement representative will forward all timely, complete, and properly formatted quotations to an evaluation committee, which the procurement representative will chair.

Committee Review of the Quotations

The State's review committee will evaluate and numerically score each quotation that the procurement representative has forwarded to it.

The evaluation will result in a point total being calculated for each quotation. Those Vendors submitting the highest-rated quotations may be scheduled for the next phase. The number of quotations forwarded to the next phase will be within the committee's discretion, but

Regardless of the number of quotations selected for the next phase, they will always be the highest rated quotations from this phase.

At any time during this phase, the State may ask a Vendor to correct, revise, or clarify any portions of its quotation.

The State will document all major decisions in writing and make these a part of the file along with the evaluation results for each quotation considered.

Once the technical merits of a quotation are considered, the costs of that quotation will be considered. But the State may also consider costs before evaluating the technical merits of the quotations by doing an initial review of costs to determine if any quotations should be rejected because of excessive cost. And the State may reconsider the excessiveness of any quotation's cost at any time in the evaluation process.

Interviews

The State may record any presentations, demonstrations and interviews.

Determination of Responsibility

The State may review the highest-ranking Vendors or its key team members to ensure that the Vendor is responsible. The Contract may not be awarded to a Vendor that is determined to be not responsible. The State's determination of a Vendor's responsibility may include the following factors: the Vendor's and its key team members' experience, past conduct on previous Contracts, past performance on previous Contracts, ability to execute this contract properly and management skill. The State will make such determination of responsibility based on the Vendor's quotation, reference evaluations and any other information the State requests or determines to be relevant.

Changing Candidates

The major criterion on which the State bases the award of the contract is the quality of the Vendor's candidate(s). Changing personnel after the award may be a basis for termination of the contract.

Contract Award Process

It is OIT's intention to award one contract under the scope of this RFQ and as based on the RFQ Calendar of Events schedule, so long as OIT determines that doing so is in the State's best interests and OIT has not otherwise changed the award date. Any award decision by OIT under this RFQ is final. After OIT makes its decision under this RFQ, all Proposers will be notified in writing of the final evaluation and determination as to their proposals.

OIT anticipates making one award depending on program needs and the fit of the Proposer to the scope of this RFQ.

ATTACHMENT ONE

VENDOR PROFILE SUMMARY

VENDOR REFERENCES

Vendor's Name:

References. Provide three references for which the proposed candidate has successfully demonstrated meeting the requirements of the RFQ on projects of similar size and scope in the past five years. The name of the person to be contacted, phone number, company, address, brief description of project size and complexity, and date (month and year) of employment must be given for each reference. These references must be able to attest to the candidate's specific qualifications.

The reference given should be a person within the client's organization and not a co-worker or a contact within the offerors organization.

If less than three references are provided, the offeror must explain why. The State may disqualify the Proposal if fewer than three references are given.

| | | | |
|---|---|--|--|
| Client Company: | Client Contact Name: | Client Contact Title: | |
| Client Address: | | Client Contact Phone Number: | |
| Project Name: | Beginning Date of Employment: Month/Year | Ending Date of Employment: Month/Year | |
| Description of services provided that are in line with those to be provided as part of this Project: | | | |
| Description of how client project size and complexity are similar to this project: | | | |

**ATTACHMENT ONE VENDOR
PROFILE SUMMARY VENDOR
REFERENCES CONTINUED**

| | | | |
|---|---|--|--|
| Client Company: | Client Contact Name: | Client Contact Title: | |
| Client Address: | | Client Contact Phone Number: | |
| Project Name: | Beginning Date of Employment: Month/Year | Ending Date of Employment: Month/Year | |
| <p>Description of services provided that are in line with those to be provided as part of this Project:</p> <p>Description of how client project size and complexity are similar to this project:</p> | | | |

| | | | |
|------------------------|---|--|--|
| Client Company: | Client Contact Name: | Client Contact Title: | |
| Client Address: | | Client Contact Phone Number: | |
| Project Name: | Beginning Date of Employment: Month/Year | Ending Date of Employment: Month/Year | |

Description of services provided that are in line with those to be provided as part of this Project:

Description of how client project size and complexity are similar to this project: