We Set the Standard for Good Government

COLORADO OFFICE OF THE STATE AUDITOR

A REQUEST FOR PROPOSALS

FOR AN EVALUATION OF WEB APPLICATION SECURITY AT THE COLORADO STATEWIDE INTERNET PORTAL AUTHORITY

April 10, 2020

TABLE OF CONTENTS

SECTION I
ADMINISTRATIVE INFORMATION

A. ISSUING OFFICE

This request for proposal (RFP) is issued by the Colorado Office of the State Auditor (OSA). The terms State Auditor, OSA, State, and State of Colorado are used interchangeably throughout this RFP.

As an agency within Colorado's Legislative Branch, the OSA and this solicitation are exempt from the State Procurement Code and State Procurement Rules [see Section 24-101-105(1)(a), C.R.S.].

All communications regarding this RFP must take place directly with the OSA's assigned contract monitor listed in Section I(E) – *Inquiries* ***and Section I(F) –*** *Submission of Proposals.*

B. BACKGROUND INFORMATION

The OSA is soliciting proposals from qualified organizations to conduct an IT performance evaluation of IT security over web applications developed, operated and maintained by the Colorado Statewide Internet Portal Authority.

Colorado Statewide Internet Portal Authority

The Colorado Statewide Internet Portal Authority, SIPA, was created by Colorado Statute (C.R.S. § 24-37.7-101 et seq.) in 2004, to develop the officially recognized statewide internet portal (Colorado.gov) to connect citizens with state and local government in Colorado. SIPA was charged to create an efficient, effective, and user friendly statewide internet portal to serve as a place where citizens can electronically access state government information, products, and services, as well as provide e-Government services to state and local governments.

The mission of Colorado SIPA is to provide efficient and effective services for citizens through the use of modern business practices and innovative technology solutions. Colorado SIPA's vision is to transform Colorado government service delivery through the use of technology, allowing a single point of contact for members of the public to access state and local government information, products, and services. Under the leadership and guidance of the executive director and board of directors, the goals of Colorado SIPA are:

- To continue development of a statewide internet portal that provides a single access point to information, products, and services of state and local

government to give members of the public an effective and efficient way to transact business

- To increase the number of applications developed, integrated, and made publicly available on the Portal by government entities

- To continue the micro-grant program for government entities to accelerate adoption of online services for their constituents

- To increase the number of eligible government entities that use the services provided by the Authority through promotion and education

- To explore and expand the type of products, services and solutions offered to governmental entities through the Authority

SIPA is the oversight body of the Colorado.gov web portal, the gateway to Colorado government. With services powered by its Portal Integrator, Colorado Interactive (CI), Colorado.gov is Colorado's single most comprehensive delivery channel for no-cost e-Government services like websites, online forms, payment processing and event registration applications.

SIPA offers no-cost setup for governments to create a website on the colorado.gov Drupal platform. The following link contains a list of all websites on the Colorado.gov platform:

- https://www.colorado.gov/goingpacific/view-all-pacific-sites

SIPA, in partnership, with CI, also offers no-cost payment processing solutions for governments to accept eChecks, online, mobile and over-the-counter payments through a secure web-based application. This application integrates with the Colorado Operations Resource Engine (CORE), which is the accounting system of final record used by most Colorado state agencies to perform day-to-day accounting and financial reporting functions for state transactions.

SIPA is governed by a Board of Directors. The Board appoints an Executive Director to oversee daily operations, and to ensure the goals and objectives of the Authority are met.

SIPA is self-funded, meaning, no tax dollars or appropriated funds are used. Under this model, other revenue sources are identified and established to fund no-cost portal offerings and competitively priced solutions. The self-funded portal remains financially viable by charging approved administrative fees on certain transaction services. The fees are then reinvested to provide micro-grants, infrastructure and services that enhance the efficiency of Colorado government interactions with citizens and businesses.

The OSA conducted a prior performance audit at SIPA that reviewed SIPA's contract

administration practices, system of internal controls over financial activities, information technology controls, and the cost-effectiveness of SIPA services. A link to this audit report has been included at the end of this document in Section IV, Supplemental Information.

State Auditor Authority

In August 2013, as noted in Section 2-3-103(1.5)(b)(I), C.R.S., the General Assembly gave the OSA the authority to assess and report on the security practices of all of the information technology systems maintained or administered by all departments, institutions, and agencies of state government, including educational institutions and the judicial and legislative branches. This includes the authority to perform ongoing vulnerability assessments and penetration tests of state agencies, including institutions of higher education.

C. SERVICES REQUIRED

The OSA is soliciting proposals from qualified organizations to conduct an IT performance evaluation of IT security over web applications developed, operated and maintained by the Colorado Statewide Internet Portal Authority. Subject to oversight and direction provided by the OSA, the engaged firm (Contractor) will be responsible for planning and conducting the evaluation to obtain sufficient, appropriate evidence necessary to conclude on the evaluation's objectives, develop complete written findings, write the report[1], and present the report to the Legislative Audit Committee (LAC).

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this IT performance evaluation is to review IT security over state websites and/or web applications and services developed, operated, and maintained by SIPA to ensure that state business conducted and/or sensitive data transmitted via state websites, applications and services are available, as needed, and protected from unauthorized access and changes. The engaged contractor will perform the engagement through a risk-based approach by selecting for review key, mission-critical state websites that enable agencies and citizens to conduct business electronically and to transmit and/or maintain sensitive information. To achieve the objective, the contractor will perform, but not be limited to, the following:

- Develop a detailed, risk-based project scope and methodology, in partnership with the OSA, to align with the overall project timelines outlined in this RFP.

[1] Two reports may be necessary to report the findings, conclusions, and recommendations associated with this evaluation. One report would be made public after being released by the LAC, and another report would remain confidential and would not be released publicly by the LAC in order to protect any sensitive information that may need to be reported in it. Any such confidential report may be presented to the LAC and/or other oversight bodies or legislative committees, through non-public, closed hearings (e.g., executive sessions), if deemed necessary and approved by the LAC and State Auditor. All further references to the evaluation "report" in this document will include the possibility of two reports.

The detailed scope will outline the select web applications, services, technologies, processes and controls that will be evaluated, as well as the detailed approach and methodology used. As such, each bidding contractor's proposal should include the planned approach and processes it will use to determine the various items to be included in the scope, as well as what would be excluded.

- Perform a web application vulnerability assessment (VA) to determine whether the selected web applications and/or services contain security vulnerabilities or issues that need remediation.

- Perform a related penetration test to exploit and demonstrate the existence of the web application vulnerabilities and risks identified in the VA.

  Note: In addition to any web application security frameworks and standards used by SIPA, the contractor should use any other industry leading web application security frameworks and/or standards, such as the National Institute of Standards and Technology's Special Publication 800-95 Guide to Secure Web Services, the Open Source Foundation for Application Security (OWASP) Top 10, or the OWASP Web Security Testing Guide (WSTG), as criteria to identify critical security risks to web applications and as a framework of best practices used by organizations to test the security of web applications and web services (i.e., to perform web application security vulnerability assessments and penetration tests).

- Perform a review of key IT and/or information security processes and controls related to secure web application development, operations and maintenance, to determine whether such processes and controls have been designed, put in place, and operate effectively to minimize web application security risks. This review will also be used to determine whether any related security process and/or control problems identified relate to the causes of any technical vulnerabilities or exploitations confirmed during the vulnerability and penetration testing assessments.

The scope will only include current, operational Colorado state websites, web applications, and web services, whether internal or external facing, and will not include SIPA developed, operated and/or maintained websites and web applications/services that are not Colorado state government websites and/or web applications/services, such as city, county or special district websites and/or web applications/services. Although the scope of the evaluation will primarily review SIPA's IT and information security related processes and controls that support the development, operations, and maintenance of the in-scope websites, web applications, and web services, it may also include a review of any related agency-owned business processes and controls. Additionally, applicable SIPA contract management practices as well as procedures to evaluate IT or information security practices of SIPA's third party vendors, contractors, and/or service providers, such

as those related to Colorado Interactive (CI), may also be included in the scope of this evaluation if deemed necessary to the achievement of the objectives of evaluation, and based on the results of the engaged contractor's planning and risk assessment procedures.

DELIVERABLES AND TIMELINES

The OSA expects the Contactor to satisfy the project deliverables and timelines outlined in this RFP to meet a March 2021 Legislative Audit Committee hearing date, at which point the evaluation report will be publicly released, with any associated confidential report being reported through a closed, non-public executive session of the LAC, and potentially one or more other oversight bodies or legislative committees (e.g., the Joint Technology Committee, the Joint Budget Committee, etc), upon request and approval of the LAC.

Work for this project is *estimated* to commence approximately the week of June 22, 2020. However, work could begin sooner or later depending on how long it takes to route and execute the contract after selection of the successful proposal. *No work can begin until the contract is approved and signed by the State Auditor or her designee.*

Planning and Fieldwork

The planning and fieldwork phases of this project are expected to take place from approximately the weeks of June 29, 2020 through September 21, 2020 and include the following project deliverables and timelines:

Planning and Fieldwork		
Tasks	**Details**	**Completed Approximately By the Week of:**
Hold Planning Meeting with the OSA	Hold a planning meeting with the OSA contract monitor prior to the entrance conference. This meeting could be held in person or by conference call.	6/29/2020
Hold Entrance Conference with SIPA	Hold an in-person entrance conference with the appropriate SIPA personnel to discuss the evaluation, timeline, and logistics. The OSA contract monitor (IT Deputy State Auditor) and State Auditor participate in this meeting. The Contractor is responsible for scheduling this meeting with the assistance of the OSA contract monitor.	7/6/2020
Execute Rules of Engagement	Prior to beginning fieldwork, the selected contractor must work with SIPA's chief information officer, or other management official performing comparable duties, or his/her delegate, to agree in writing to any rules governing the manner in which the testing or assessment is to be conducted, including a mitigation plan for handling significant system outages or disruptions in the event they occur.	7/13/2020

Planning and Fieldwork		
Tasks	**Details**	**Completed Approximately By the Week of:**
Begin Fieldwork	Obtain and review documentation, interview SIPA personnel and others as appropriate, and analyze data. Have ongoing communication with SIPA throughout fieldwork to request documentation and data; ensure a clear understanding of operations, requirements, and criteria; clear the results of file reviews and data analysis; and update on logistics.	7/27/2020
Provide Updates to the OSA	Provide routine updates regarding the status of the work, noted problems, preliminary findings, etc. to the OSA contract monitor throughout the duration of the engagement. The Contractor must notify the OSA contract monitor immediately of any problems or delays in gathering information, completing the work, or communicating with SIPA. Routine updates may be provided verbally and/or through written progress reports on a schedule determined jointly by the OSA contract monitor and the Contractor.	Starting approximately the week of 8/3/2020 and ongoing bi-weekly through the completion of the contract, or more frequently, as necessary.
Complete Fieldwork	The primary fieldwork necessary to conclude on the objectives and support the findings should be substantially complete by this date. Any exceptions or issues noted during fieldwork should be appropriately cleared with SIPA before any associated findings are developed.	9/21/2020

Findings & Reporting

The OSA has a rigorous findings and report review process, which includes review and revisions at multiple levels of the organization as well as review and comment by SIPA. Prospective bidders should take this into consideration when preparing a proposed calendar and budget. The findings must adhere to the OSA's standards as described in "Exhibit G – Developing and Presenting Findings" of the OSA's standard contract, which is included in Section IV – Supplemental Information. The final report, including any associated confidential report, must adhere to the OSA's standards as described in "Exhibit H – Reporting Requirements and Format for Separately Issued Reports" of the OSA's standard contract, which is included in Section IV – Supplemental Information.

Section IV – Supplemental Information also includes links to examples of recent reports issued by the OSA. Prospective bidders should review that example report to gain an understanding of the OSA's high expectations in terms of form and presentation and, more importantly, the quality of the evidence that is used to develop and substantiate the findings and conclusions.

The findings and reporting phase of this project is expected to take place from approximately the weeks of September 21, 2020 through March 2, 2021 and includes the following project deliverables and timelines:

Findings and Reporting		
Tasks	**Details**	**Completed No Later Than**
Submit Written Draft Findings to the OSA Contract Monitor	Prepare and submit detailed written findings reflecting completion of all the work required in the scope of work to the OSA contract monitor. The findings must adhere to the format outlined in "Exhibit G – Developing and Presenting Findings" of the OSA's standard contract. The Contractor should allow approximately 3 weeks for review by the OSA contract monitor and for the Contractor to make revisions. If needed, the Contractor and OSA contract monitor will schedule a meeting or conference call to discuss the draft findings. *Adjustments and refinements to the project schedule may occur as the draft written findings are discussed, reviewed, revised.*	9/21/2020
Coordinate with the OSA Contract Monitor to Submit Written Findings to the State Auditor	The Contractor should allow a minimum of 2 weeks for the State Auditor's review and for the Contractor to make revisions. If needed, the OSA contract monitor will schedule a meeting or conference call for the Contractor to discuss the findings with the State Auditor. *Adjustments and refinements to the project schedule may occur as the draft written findings are discussed, reviewed, revised.*	10/12/2020
Coordinate with the OSA Contract Monitor to Submit Written Findings to SIPA	Once the written findings are approved by the State Auditor, coordinate with the OSA contract monitor to submit the written findings to SIPA for review prior to the findings clearing meeting. The written findings should be provided to SIPA at least 1 week prior to the findings clearing meeting. *Adjustments and refinements to the project schedule may occur as the draft written findings are discussed, reviewed, revised.*	10/26/2020
Hold Findings Clearing Meeting with SIPA	Hold an in-person findings clearing meeting with SIPA to discuss SIPA's feedback on the written draft findings. The OSA contract monitor participates in this meeting. The Contractor is responsible for scheduling this meeting with the assistance of the OSA contract monitor, if needed. The Contractor should also anticipate holding additional findings meetings to brief the audited agencies' oversight bodies (e.g., Boards, Commissions, Committees, etc.), if necessary. The engaged contractor should attend these meetings in person.	11/2/2020
Prepare Draft Report	Prepare a draft report using the written findings and the requirements outlined in "Exhibit H – Reporting Requirements and Format for Separately Issued Reports" of the OSA's standard contract. As noted, due to the nature of the evaluation, there may likely be two evaluation reports: one that will contain findings and recommendations that will be released by the LAC as a public report, and one that will remain confidential. The State Auditor and contract monitor will assist in making this determination.	11/9/2020

Findings and Reporting		
Tasks	**Details**	**Completed No Later Than**
Submit Draft Report to the OSA	Submit the draft report to the OSA contract monitor for review. Allow approximately 3 weeks for the OSA contract monitor and State Auditor to review the draft report, and for the Contractor to make revisions in response to those reviews.	11/23/2020
Submit Draft Report to SIPA	Once the draft report is approved by the State Auditor, coordinate with the OSA contract monitor to submit the draft report to SIPA for review prior to the exit conference and begin preparing its written responses to any recommendations. The draft report should be provided to SIPA at least 1 week prior to the exit conference.	12/28/2020
Hold Exit Conference with SIPA	Hold an in-person exit conference with SIPA to obtain and discuss feedback on the draft report and SIPA's planned responses to any recommendations. The Contractor is responsible for scheduling this meeting with the assistance of the OSA contract monitor, if needed. In consultation with the OSA, the Contractor is responsible for making revisions to the report, as appropriate, to address comments or concerns raised by SIPA. All report changes must be reviewed and approved by the OSA before submitting the revised draft to SIPA.	1/4/2020
Obtain Written Responses from SIPA	Coordinate with the OSA contract monitor to obtain and review SIPA's written responses to recommendations and, once obtained, work with the OSA to revise the report narrative, suggest revisions to SIPA's responses, and prepare Auditor's Addenda, as appropriate (i.e., for any disagreement or partial agreement from SIPA to the reported recommendations).	1/11/2020
Final Report Review and Approval for Print	Review the final report to ensure the accuracy of all information contained in the report. Submit the final print-ready report to the OSA contract monitor for final review and approval by the OSA contract monitor and State Auditor.	Submit final print-ready report to the OSA no later than approximately the week of 1/18/2020. OSA to provide approval to print no later than approximately 2/12/2020.

Findings and Reporting		
Tasks	**Details**	**Completed No Later Than**
Provide Final Electronic Report File and Printed Hard Copies to the OSA	Once the State Auditor has approved the final report for printing, provide the OSA contract monitor with the following: o An electronic copy of the final report file in *unprotected* PDF format. o Up to 100 hard copies of the bound printed report, or reports, if a confidential report is also produced. The exact number of copies will be determined by the OSA at the time of report finalization. Acceptable binding formats are limited to spiral, comb, and glued bindings; 3-ring bindings are not acceptable. The OSA is responsible for distributing the final report to the Legislative Audit Committee and SIPA in advance of the hearing.	2/15/2020
Conduct Dry Run of LAC Presentation with the OSA	Coordinate with the OSA contract monitor regarding the format and content of the Legislative Audit Committee presentation, and any other oversight body or legislative committee presentation requested and deemed necessary. This includes conducting a dry run of the Contractor's presentation with the OSA contract monitor and incorporating suggested revisions. The dry run can occur in person or via conference call. The Contractor may also be asked to provide the OSA with a written script of the presentation.	2/15/2020
Present Report to the Legislative Audit Committee	Provide in-person oral testimony to the Legislative Audit Committee, and potentially other oversight bodies or legislative committees (e.g., Joint Technology Committee, SIPA's Board of Directors, etc.), if requested and approved. The Contractor will be required to testify for about 1½ to 2 hours, summarizing the report's findings, conclusions, and recommendations and responding to questions from Committee members.	3/2/2020

D. SCHEDULE

The following schedule will be followed with respect to this RFP: Week of:

1.	RFP available to prospective bidders	4/10/2020
2.	Prospective bidder's inquiry deadline (5:00 p.m. MT)	4/20/2020
3.	OSA response to inquiries deadline	5/8/2020
4.	**Proposal submission deadline (5:00 p.m. MT)**	**5/15/2020**
5.	Interviews with presentations by top candidates* **Interviews are optional based on State Auditor's discretion*	6/8/2020
6.	Approximate bid selection date	6/15/2020
7.	Approximate contract date	6/22/2020

E. INQUIRIES

Prospective bidders may make written inquiries concerning this RFP to obtain clarification of requirements. Inquiries must be submitted via email to Matt Devlin, Contract Monitor, at matt.devlin@state.co.us. ***No inquiries will be accepted after 5:00 p.m. MDT on 4/20/2020.***

F. SUBMISSION OF PROPOSALS

Proposals must be submitted via email to Matt Devlin, Contract Monitor, at matt.devlin@state.co.us. ***No proposal submissions will be accepted after 5:00 p.m. MDT on 5/15/2020.***

All proposals become the property of the State Auditor upon receipt and will not be returned to the bidder. The State Auditor shall have the right to use all ideas, or adaptations of these ideas, contained in any proposal received in response to this RFP. Selection or rejection of the proposal will not affect this right.

G. ACCEPTANCE OF PROPOSAL

This RFP does not commit the State Auditor to award a contract, to pay any costs incurred in the preparation of a bid submitted in response to this request, or to procure or contract for services or supplies. The State Auditor reserves the right to accept or reject, in part or in its entirety, any or all bids received as a result of this RFP if, in the opinion of the State Auditor, it is in the best interest of the State to do so. The lowest cost proposal will not necessarily be selected. The State Auditor also reserves the right to engage in further negotiation of the project scope, price, and contract terms after selection of the Contractor if, in the opinion of the State Auditor, it is in the best interest of the State to do so.

H. ADDENDUM OR SUPPLEMENT TO REQUEST FOR PROPOSAL

The State Auditor reserves the right to issue amendments to this RFP prior to the closing date for submission of proposals. In the event that it becomes necessary to revise any part of this RFP, an addendum to this RFP will be provided to each prospective bidder.

I. AWARD WITHOUT DISCUSSION

The State Auditor reserves the right to make an award without further discussion of proposals received. Therefore, proposals must be submitted in the most complete terms possible from both the technical and cost standpoint.

J. AWARD INFORMATION TO UNSUCCESSFUL FIRMS

The State Auditor will notify all unsuccessful bidders after the award. No information will be released after the proposal submission deadline until an award

has been made.

K. JOINT VENTURES

No joint venture proposals will be accepted. However, this requirement does not preclude the use of outside special consultants if deemed necessary by the Contractor.

L. STATE AUDITOR LIAISON

The OSA's assigned contract monitor will be the liaison to the Contractor throughout the project. This individual will attend entrance/exit conferences and assist the Contractor in understanding the OSA's requirements, processes, and expectations.

M. AWARD OF BID

The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered. The successful bidder will be awarded a contract for the scope detailed in this RFP or the scope negotiated through further discussion.

N. SUBMISSION OF INVOICES

The Contractor must submit monthly invoices for work completed. The State Auditor will withhold 10 percent of the total contract amount pending satisfactory completion of the contract scope of work.

SECTION II
INFORMATION THAT MUST BE INCLUDED IN PROPOSAL

All proposals ***must*** include the information requested in this section and be organized in the same manner as this section.

Proprietary Information: All proposals submitted to the OSA in response to this RFP are subject to the Colorado Open Records Act (CORA). ***Any proprietary information included in the proposal must be clearly and specifically designated as such in the proposal.*** The OSA will redact proprietary information from the proposal pursuant to 24-72-204(3)(a)(IV), C.R.S., allowing for the denial of inspection of records including trade secrets, before providing the proposal in response to a CORA request.

A. TITLE PAGE

The proposal will identify the RFP subject, organization's name, address, telephone number, name of contact person, and date.

B. TABLE OF CONTENTS

The proposal will include a clear identification of the material included in the bid proposal by section and page number.

C. TRANSMITTAL LETTER

Please limit the transmittal letter to no more than two pages. Provide the names of individuals authorized to make representations for the organization and their titles, addresses, and telephone numbers.

D. PROFILE OF THE ORGANIZATION

The proposal must:

1. State whether the organization is local, national, or international.

2. Give the location(s) of the office from which the work will be done and number of partners, shareholders, and managers and other professional staff employed at that office.

3. Describe the range of activities performed by the office from which the work will be done, including descriptions of or links to prior work products that demonstrate experience and expertise providing the services described in this RFP.

4. Describe any and all (a) work that is currently being performed for SIPA or the State of Colorado, (b) work that was performed for SIPA or the State of Colorado

within the past 2 years (i.e., *April 2018 – April 2020*), and (c) planned work for SIPA or the State of Colorado (i.e., proposals submitted for work that has not yet been awarded or contracted).

5. Affirm that the organization is independent for this engagement.

   Prior, current, or planned work disclosed pursuant to Item #4 may create a threat to independence. In affirming the organization's independence for this engagement, the proposal must include explanation/analysis why this prior, current, or planned work would not impair the organization's independence—or create the appearance thereof—in performing this evaluation of SIPA.

6. Affirm that the organization does not have any past history of substandard work (e.g., a prior engagement has been terminated for poor performance).

7. Provide information on any past, current, or anticipated claims (i.e., knowledge of pending claims) on respondent contracts; explain the litigation, the issue, and its outcome or anticipated outcome.

8. Provide no more than three references for similar work performed.

E. QUALIFICATIONS OF ASSIGNED PERSONNEL

Describe the proposed evaluation team's relevant experience and areas of expertise. The proposal must identify the principal staff (i.e., principals, managers, and supervisors/in-charges) who will work on the evaluation, including any specialists or subcontractors to be used. The proposal must include a resume of all principal staff highlighting their professional qualifications and similar evaluation work that they have performed. Resumes must be included in an appendix.

The OSA *may* require that the Contractor provide the OSA with the results of background checks conducted pursuant to the organization's standard employment practices on personnel assigned to the engagement. If background checks are not a standard employment practice for the Contractor, the OSA *may* require the Contractor to conduct a background check on personnel assigned to the engagement and provide the results to the OSA.

F. ORGANIZATION'S APPROACH TO THE EVALUATION

The proposal must include a description of the methodology, approach, tools, and resources to be used to conduct the evaluation. The proposal must set forth the steps that the organization will take to conclude on each of the objectives outlined in this RFP and ensure fully developed findings based on sufficient, appropriate evidence.

G. CONTRACT TERMS AND CONDITIONS

The OSA expects the successful bidder to execute and adhere to the terms and conditions in the OSA's standard contract and its related exhibits. The OSA's standard contract and its related exhibits are included in Section IV – Supplemental Information.

Bidders should not wait until after the OSA has made a contract award to first consult with their legal team/advisor about the contract terms and conditions. Any questions or issues with the terms and conditions in the OSA's standard contract and its related exhibits must be identified and described as part of the proposal, including alternative language the bidder is proposing. ***The OSA will consider this information when evaluating proposals and making the contract award.***

H. COMPENSATION

1. The proposal must state the number of professional staff hours estimated to complete the work by staff level, the hourly rate, and the resulting total cost. Travel costs incurred in the performance of evaluations are reimbursable only as a part of the hourly rate and must be covered under said rate and will not be separately reimbursed.

2. The proposal must break out total hours estimated to (a) complete each issue/objective/question and (b) write and revise findings and the final report.

3. The proposal must state the total inclusive maximum fee for which the work requested will be done.

4. The proposal must affirm that all prices, terms, and conditions will be held firm for at least 90 days after the bid opening.

I. DELIVERY SCHEDULE

The proposal must include a detailed proposed schedule of the work to be performed and deliverable due dates for the project milestones discussed in Section I(C) – Services Required.

J. ADDITIONAL DATA

The organization may include additional information in this section that is considered essential to the proposal, *but has not been specifically provided in response to prior sections of this RFP*.

SECTION III
PROPOSAL EVALUATION PROCESS

A. GENERAL

An OSA evaluation team will judge the merits of proposals received in accordance with the general criteria defined below. The bidder is responsible for providing all information requested in this RFP. Failure to do so may result in disqualification of the proposal.

The evaluation team will select the bidder whose proposal is most responsive to the State Auditor's needs while being within available resources. The specifications within this RFP represent the minimum performance necessary for response.

During the evaluation process, the evaluation team may, at its discretion, request any one or all bidders to make oral presentations or answer questions about their proposals. Not all bidders may be asked to make such oral presentations.

B. MANDATORY CRITERIA

1. The organization is independent for the engagement.

C. GENERAL CRITERIA

1. Adequacy and completeness of the proposal with regard to Section II of the RFP.

2. Experience and stability of the organization.

3. Qualifications and experience of staff, including subcontractors, specialists, and consultants to be assigned to the evaluation.

4. Comprehensiveness and appropriateness of the proposed work plan.

5. Proposed hours and cost.

6. Proposed time frame for meeting project milestones and completing the evaluation.

7. Willingness to execute/accept the OSA's standard contract and its related exhibits without significant revision and negotiation.

D. TOTAL SCORE

The evaluation team will assign scores to the proposals based on the established criteria. The State Auditor will make the final decision on the contract award.

SECTION IV
SUPPLEMENTAL INFORMATION

Attached to this RFP is the following document:

1. Standard OSA contract and related exhibits. See Section II(G) of the RFP for discussion.

The following web links references provide additional information to assist in preparing the proposal:

- Statewide Internet Portal Authority's (SIPA) Website: https://sipa.colorado.gov/

- State of Colorado Governor's Office of Information Technology (OIT) Website: http://www.colorado.gov/oit

- Colorado Office of the State Auditor Website: http://www.colorado.gov/auditor

- OSA IT Performance Evaluation Report Example: Evaluation of IT Security at the Colorado Department of Transportation, Public Report, February 2020. http://leg.colorado.gov/audits/evaluation-information-technology-security-colorado-department-transportation

- OSA IT Performance Audit Report Example: Audit of Three IT Systems at the Colorado Department of Public Health and Environment, IT Performance Audit, Public Report, August 16, 2017 http://leg.colorado.gov/audits/audit-three-information-technology-systems-colorado-department-public-health-and-environment

- OSA IT Performance Audit Report Example: Audit of the Information Security of the Colorado Operations Resource Engine (CORE) System, IT Performance Audit, Public Report, April 25, 2016 http://leg.colorado.gov/audits/audit-information-security-colorado-operations-resource-engine-core-system

- OSA IT Performance Evaluation Report Example: Information System Security Assessment, Governor's Office of Information Technology and Judicial Branch, IT Performance Evaluation, Public Report, November 2014 http://leg.colorado.gov/audits/it-vulnerability-assessment

- OSA Performance Evaluation Report Example: Statewide Internet Portal Authority, Performance Audit, November 2012

http://leg.colorado.gov/audits/statewide-internet-portal-authority

- State Auditor's Statutory Authority To Conduct IT Security Evaluations:

This evaluation will be conducted under the authority of Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government; and Section 2-3-103(1.5) et seq., C.R.S., which states:

> (1.5) (a) In addition to any other duties granted by law, the state auditor may assess, confirm, and report on the security practices of all of the information technology systems maintained or administered by all departments, institutions, and agencies of state government, including educational institutions and the judicial and legislative branches. The auditor may perform similar or related duties with respect to political subdivisions of the state where the auditor has been granted authority to perform financial or performance audits with respect to such political subdivisions. In order to perform such duties, the state auditor may conduct penetration or similar testing of computer networks or information systems of the state or a political subdivision, as applicable, assess network or information system vulnerability, or conduct similar or related procedures to promote best practices with respect to the confidentiality, integrity, and availability of information systems technology as the auditor deems necessary in his or her discretion. In conducting such testing, the state auditor may contract with auditors or information technology security specialists, or both, that possess the necessary specialized knowledge and experience to perform the required work. The authority of the state auditor pursuant to the requirements of this subsection (1.5) shall be coextensive with the auditor's authority under this part 1.
>
> (b) Any testing or assessment of security practices and procedures concerning information technology in accordance with paragraph (a) of this subsection (1.5) shall be conducted or caused to be conducted by the state auditor:
>
> > (I) After consultation and in coordination with, but not requiring the approval of, the chief information officer appointed pursuant to Section 24-37.5-103, C.R.S., or any person performing comparable duties for either a state agency that is not under the jurisdiction of the office of information technology created in Section 24-37.5-103, C.R.S., or a political subdivision of the state;

(II) In accordance with industry standards prescribed by the National Institute of Standards and Technology or any successor agency; and

(III) After the state auditor and any other person with whom the state auditor is required to consult in accordance with the requirements of subparagraph (I) of this paragraph (b) have agreed in writing to rules governing the manner in which the testing or assessment is to be conducted, including a mitigation plan for handling significant system outages or disruptions in the event they occur.

Routing # 20XX-XX

STATE OF COLORADO
State Auditor and
Legislative Audit Committee
Performance Evaluation Contract for the
Evaluation of the INSERT NAME OF ENTITY
With
INSERT NAME OF CONTRACTOR

TABLE OF CONTENTS

1. PARTIES

This Contract ("Contract") is entered into by and between [insert contractor's name] ("Contractor"), and the STATE OF COLORADO (the "State") acting by and through and for the use and benefit of the State Auditor and the Legislative Audit Committee. Contractor and the State agree to the following terms and conditions specified in this contract.

2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

The Effective Date of this Contract is the date on which this Contract has been approved and signed by all of the Parties, including on behalf of the State the State Auditor or the State Auditor's designee and the Chair of the Legislative Audit Committee, and also signed, after legal review, by the Director of the Office of Legislative Legal Services or the Director's designee. This Contract is not effective or enforceable before the Effective Date, and the State is not liable to pay or reimburse Contractor for any Work performed or costs or expenses incurred by the Contractor before the Effective Date or after the expiration or other termination of this Contract.

3. RECITALS

A. Authority, Appropriation, And Approval

Authority to enter into this Contract exists in §2-3-103(1), C.R.S., funds have been budgeted, appropriated, and otherwise made available pursuant to Fund 1000, Appropriation Code MGFCC4010, Contract Encumbrance Number 20XX-XX, and a sufficient unencumbered balance of the funds remains available for payment. Required approvals, clearance, and coordination have been accomplished from and with appropriate agencies.

B. Consideration

The Parties acknowledge that the mutual promises and covenants contained in this Contract, including the Exhibits attached to and incorporated by reference in this Contract are sufficient and adequate to support this Contract.

C. Purpose

The State is engaging Contractor to render professional evaluation services as specified in this Contract, including the Exhibits attached to and incorporated by reference into this Contract.

4. DEFINITIONS

The following terms shall be construed and interpreted as follows:

A. Agency

"Agency" means the [insert department/agency name].

B. Business Day

"Business Day" means any day on which the State is open and conducting business, but does not include Saturday, Sunday, or any day on which the State observes a legal holiday listed in §24-11-101(1), C.R.S.

C. CJI

"CJI" means criminal justice information collected by criminal justice agencies needed for the performance of their authorized functions, including, without limitation, all information defined as criminal justice information by the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy and all criminal justice records, as defined in §24-72-302, C.R.S.

D. Contract

"Contract" means this Contract, including the Exhibits attached to and incorporated by reference into this Contract, any other documents incorporated by reference into this Contract, and any amendments to this Contract or additional Exhibits or other documents incorporated into this Contract after the Effective Date.

E. Contract Funds

"Contract Funds" means the maximum amount of funds available for payment by the State to Contractor pursuant to **§7(A)** of this Contract.

F. CORA

"CORA" means the "Colorado Open Records Act", §§24-72-200.1, *et seq.,* C.R.S.

G. Effective Date

"Effective Date" means the date on which this Contract has been approved and signed by all of the Parties and, after legal review, by the Director of the Office of Legislative Legal Services or the Director's designee.

H. Evaluation Report

"Evaluation Report" means the final performance evaluation report due to the State in accordance with this Contract.

I. Exhibits

"Exhibits" means the following Exhibits that are attached to and incorporated by reference into this Contract: **Exhibit A** (Statement of Work), **Exhibit B** (Request for Proposal), **Exhibit C** (Modifications to Contractor's Proposal), **Exhibit D** (Contractor's Proposal), **Exhibit E** (Information Security Policy for Contractors), **Exhibit F** (Compensation and Procedures for Billing), **Exhibit G** (Developing and Presenting Findings), **Exhibit H** (Reporting Requirements and Format for Separately Issued Reports), and **Exhibit I** (Safeguarding Requirements for Federal Tax Information).

J. Incident

"Incident" means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of any communications or information resources of the State, which are included as part of the Work, as described in §§24-37.5-401, *et seq.*, C.R.S. Incidents include, without limitation, (i) successful attempts to gain unauthorized access to a State system or State Confidential Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent.

K. OSA

"OSA" means the Office of the State Auditor.

L. Party or Parties

"Party" means the State or Contractor and "Parties" means both the State and Contractor.

M. PCI

"PCI" means any payment card information including any data related to credit card holders' names, credit card numbers, or the other credit card information as may be protected by state or federal law.

N. PHI

"PHI" means any protected health information, including, without limitation, any information, whether oral or recorded in any form or medium that: (i) relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (ii) either identifies the individual or provides a reasonable basis to believe that it can be used to identify the individual. PHI includes, but is not limited to, any information defined as Individually Identifiable Health Information by the federal Health Insurance Portability and Accountability Act.

O. PII

"PII" means personally identifiable information including, without limitation: (i) any information maintained by the State about an individual that can be used to distinguish or trace the individual's identity, such as name, social security number, date and place of birth,

mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, all information defined as personally identifiable information in §24-72-501 and 24-73-101, C.R.S.

P. Proposal

"Proposal" means Contractor's Proposal dated [insert date]. [If applicable, add: ", including the modification(s) to the proposal dated [insert date(s)].]

Q. Request for Proposal or RFP

"Request for Proposal" or "RFP" means the State's Request for Proposal issued [insert date]. [If applicable, add: ", including the supplement(s) to the RFP dated [insert date].]

R. Services

"Services" means the required performance evaluation services to be performed by Contractor pursuant to this Contract.

S. State Auditor

"State Auditor" means the Colorado State Auditor.

T. State Confidential Information

"State Confidential Information" means any and all State Records not subject to disclosure under CORA. State Confidential Information includes, but is not limited to, PII, PHI, PCI, Tax Information, CJI, and State personnel records not subject to disclosure under CORA. State Confidential Information does not include information or data concerning individuals that is not deemed confidential but nevertheless belongs to the State, that has been communicated, furnished, or disclosed by the State to Contractor and that: (i) is subject to disclosure pursuant to CORA; (ii) is already known to Contractor without restrictions at the time of its disclosure to Contractor; (iii) is or subsequently becomes publicly available without breach of any obligation owed by Contractor to the State; (iv) is disclosed to Contractor, without confidentiality obligations, by a third party who has the right to disclose such information; or (v) was independently developed without reliance on any State Confidential Information.

U. State Fiscal Rules

"State Fiscal Rules" means the fiscal rules promulgated by the Colorado State Controller pursuan to §24-30-202(13)(a), C.R.S.

V. State Fiscal Year

"State Fiscal Year" means a 12-month period beginning on July 1 of each calendar year and ending on June 30 of the following calendar year. If a single calendar year follows the term, then the term means the State Fiscal Year ending in that calendar year.

W. State Records

"State Records" means any and all State data, information, and records, regardless of physical form, including, but not limited to, information subject to disclosure under CORA.

X. Subcontractor

"Subcontractor" means a third party, if any, engaged by Contractor to aid in performance of its obligations.

Y. Tax Information

"Tax Information " means federal and State tax information including, without limitation, federal and State tax returns, return information, and such other tax-related information as may be protected by federal and State law and regulation. Tax Information includes, but is not limited to, all information defined as Federal Tax Information (FTI) in Internal Revenue Service Publication 1075.

Z. Work

"Work" means the tasks and activities that Contractor is required to perform to fulfill its obligations under this Contract, including the performance of the Services and delivery of the Work Product.

AA. Work Product

"Work Product" means the tangible and intangible results of the Work, whether finished or unfinished, including drafts. Work Product includes, but is not limited to, documents, text, software (including source code), research, reports, proposals, specifications, plans, notes, studies, data, images, photographs, negatives, pictures, drawings, designs, models, surveys, maps, correspondence, communication, materials, ideas, concepts, know-how, and any other results of the Work. Work Product also includes the Evaluation Report, findings, oral testimony, and workpapers, whether referred to in relevant statutes as "workpapers" or "work papers," subject to **§18** of this Contract, and any separate report issued as specified in **Exhibit H**.

BB. Terms Defined in Exhibits

Any term used in this Contract that is defined in an Exhibit shall be construed and interpreted as defined in the Exhibit.

5. TERM AND EARLY TERMINATION

A. Term-Work Commencement

The Parties' respective performances under this Contract shall commence on the Effective Date. This Contract terminates on the earlier of thirty (30) days after the Evaluation Report has been released by the Legislative Audit Committee or [insert date], unless sooner terminated as specified in this Contract. The State may terminate this Contract for its convenience for any reason, without penalty to the State, upon thirty (30) days prior written notice to Contractor.

B. Early Termination

Upon early termination, Contractor shall not incur further obligations or render further performance under this Contract past the effective date of the notice of termination and shall terminate outstanding subcontracts with Subcontractors. Contractor shall deliver to the State all Work Product to the extent completed as of the termination date. Contractor shall take timely, reasonable, and necessary action to protect and preserve property in the possession of Contractor. Contractor shall immediately return to the State all materials owned by the State in the possession of Contractor in which the State has an interest. The State shall reimburse Contractor for accepted performance up to the termination date.

C. Background Checks

Notwithstanding **§5(A)**, the OSA may require Contractor, before commencing its performance under this Contract, to provide to the OSA at Contractor's own expense the results of background checks conducted pursuant to Contractor's standard employment practices for any personnel assigned to perform Work under this Contract. If Contractor does not conduct employee background checks as a standard employment practice, the OSA may require Contractor, before commencing its performance under this Contract and at Contractor's own expense, to conduct background checks on personnel assigned to the engagement and provide the results of the background checks to the OSA. In addition, a background check for an employee of Contractor whose employment by Contractor in performing the Work will allow the employee to access or use Tax Information or will otherwise subject the employee to the requirements specified in Internal Revenue Service Publication 1075 must satisfy all background check requirements set forth in both that publication and Exhibit I.

6. STATEMENT OF WORK

A. Completion

Contractor shall complete the Work on or before [insert date].

B. Services and Work Product

Contractor shall provide the Services and deliver the Work Product necessary to complete the Work. Contractor shall accomplish the provision of Services and delivery of Work Product using the Contract Funds only.

C. Employees

All persons employed by Contractor or Subcontractors to perform Work under this Contract are Contractor's or Subcontractors' personnel for all purposes of this Contract and are not employees of the State for any purpose as a result of this Contract.

7. PAYMENTS TO CONTRACTOR

The State, in accordance with the provisions of this **§7**, shall pay Contractor in the amounts and using the methods set forth below:

A. Maximum Amount

The maximum amount payable under this Contract to Contractor by the State is $[insert amount], as determined by the State from available funds. Payments to Contractor are limited to the unpaid obligated balance of the Contract and shall be made as set forth in **Exhibit F** (Compensation and Procedures for Billing). The estimated amount payable by the State to Contractor during State Fiscal Year 20XX-20XX is $[insert amount], and the estimated amount payable by the State to Contractor during State Fiscal Year 20XX-20XX is $[insert amount]. The exact funding split between the State Fiscal Years, if applicable, will be determined by the State based on amounts that have been budgeted, appropriated, or otherwise made available for this Contract.

B. Payment

i. Interim and Final Payments

Contractor shall initiate any payment requests by submitting invoices to the State in a form approved by the State and in the manner specified in **Exhibit F**. Contractor shall not request payment from the Agency.

ii. Interest

The State shall fully pay each invoice within forty-five (45) days of its receipt if the amount invoiced represents performance by Contractor previously accepted by the State. Uncontested amounts not paid by the State within forty-five (45) days bear interest on the unpaid balance beginning on the 46th day at the rate of one percent per month until paid in full. Interest does not accrue on unpaid amounts that are subject to a good faith dispute between Contractor and the State. Contractor shall invoice the State separately for accrued interest on delinquent amounts, and any such separate billing shall reference the delinquent payment, the number of days' interest to be paid, and the one percent interest rate.

C. Use of Funds

Contract Funds shall be used only for costs identified in this Contract.

8. REPORTING - NOTIFICATION

Reports required under this **§8** shall be in the form and subject to the procedures prescribed by the State.

A. Performance, Progress, Personnel, and Funds

Contractor shall comply with all reporting requirements set forth in the Exhibits.

B. Litigation Reporting

Upon being served in an action before a court or an administrative decision making body with any pleading that is related to this Contract or that may affect Contractor's ability to perform its obligations under this Contract, Contractor, within ten (10) days, shall notify the State of the action and deliver copies of the pleadings to the State's principal representative as identified in **§17** of this Contract. If the State's principal representative is not then serving, Contractor shall deliver notice and copies to the State Auditor.

C. Noncompliance

Contractor's failure to provide reports, notification of legal action, or copies of pleadings to the State in a timely manner in accordance with this **§8** may result in the delay of payment of funds, termination, or both, as provided under this Contract.

D. Subcontracts

Contractor shall submit copies of any and all subcontracts entered into by Contractor to perform its obligations under this Contract to the State or its principal representative upon request by the State.

9. CONTRACTOR RECORDS

A. Maintenance

Except as otherwise required with respect to State Records following the expiration or termination of this Contract by **§10(C)** of this Contract, Contractor shall maintain a complete file of all documents, records, communications, notes, and other materials, including but not limited to all Work Product, pertaining in any manner to the Work or the delivery of Services, including Work performed and Services delivered by Subcontractors. Unless Contractor receives written notice of an extension from the State, the federal government, or another duly authorized agent of a governmental agency, Contractor shall maintain the records until the last to occur of: (i) the date five (5) years after the date on which the State accepts the Audit Report or, in the case of early termination, terminates this Contract; (ii) the date on which any pending disputes relating to this Contract are resolved; or (iii) if the performance of this Contract is being audited or Contractor receives notice that an audit is pending, the date on which the audit is completed and its findings have been resolved (the "Record Retention Period").

B. Inspection

Contractor, at no additional charge, shall permit the State or its authorized agent(s), any successor auditor, the federal government, and any other duly authorized agent of a governmental agency to access and inspect, excerpt, and copy Contractor's work papers and reports related to this Contract during the Record Retention Period to assure compliance with the terms of this Contract, to evaluate performance under this Contract, or for any other purpose required by the State. The State reserves the right to inspect the Work at all reasonable times and places during the term of this Contract, including any extensions or renewals.

C. Monitoring

The State, in its discretion, may monitor Contractor's performance of its obligations under this Contract using procedures determined by the State that do not unduly interfere with Contractor's performance of the Work.

10. WORK PRODUCT-CONFIDENTIAL INFORMATION-STATE RECORDS

A. Confidentiality

Contractor shall keep confidential, and cause all Subcontractors to keep confidential, all State Records, unless those State Records are publicly available. Contractor shall not, without prior written approval of the State, use, publish, copy, disclose to any third party, or permit the use by any third party of any State Records, except as otherwise stated in this Contract, permitted by law, approved by the State in accordance with §2-3-103(3), C.R.S., or otherwise approved in writing by the State. Contractor shall provide for the security of all State Confidential Information in accordance with all applicable laws, rules, policies, publications, and guidelines. If Contractor or any of its Subcontractors will or may receive the following types of data, Contractor or its Subcontractors shall provide for the security of such data according to the following: **(i)** to the extent Contractor receives, transmits, processes, and/or stores Federal Tax Information (FTI) on behalf of the State, the most recently promulgated IRS Publication 1075 for all Federal Tax Information and in accordance with the Safeguarding

Requirements for Federal Tax Information attached to this Contract as an Exhibit, **(ii)** the most recently updated PCI Data Security Standard from the PCI Security Standards Council for all PCI, **(iii)** the most recently issued version of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Security Services Policy for all CJI, and **(iv)** the federal Health Insurance Portability and Accountability Act for all PHI. Contractor shall immediately forward any request or demand for State Records to the State's principal representative.

B. Other Entity Access and Nondisclosure Agreements

Contractor may provide State Records to its agents, employees, assigns, and Subcontractors as necessary to perform the Work, but shall restrict access to State Confidential Information to those agents, employees, assigns, and Subcontractors who require access to perform their obligations under this Contract. Contractor shall ensure that all such agents, employees, assigns, and Subcontractors sign agreements containing nondisclosure provisions that are at least as protective as those in this Contract, and that the nondisclosure provisions are in force at all times at which the agent, employee, assign, or Subcontractor has access to any State Confidential Information. Contractor shall provide copies of the signed nondisclosure provisions to the State upon execution of the nondisclosure provisions.

C. Use, Security, and Retention

Contractor shall use, hold and maintain State Confidential Information in compliance with any and all applicable laws and regulations in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. Contractor shall provide the State with access, subject to Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of State Confidential Information and evaluating security control effectiveness. Upon the expiration or termination of this Contract, Contractor shall return State Records provided to Contractor or if specifically instructed to do so by the State, destroy the State Records and certify to the State that it has done so as directed by the State. If any law, regulation, or other provision of this Contract prevents Contractor from returning or destroying State Confidential Information, Contractor warrants that it will guarantee the confidentiality of, and cease to use, the State Confidential Information.

D. Incident Notice and Remediation

If Contractor becomes aware of any Incident, it shall notify the State as soon as permitted and in accordance with applicable law and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the State. Unless Contractor can establish that none of Contractor or any of its agents, employees, assigns or Subcontractors are the cause or source of the Incident, Contractor is responsible for the cost of notifying each person who may have been impacted by the Incident. After an Incident, Contractor shall take steps to reduce the risk of incurring a similar type of Incident in the future as directed by the State, which may include, but is not limited to, developing and implementing a remediation plan approved by the State at no additional cost to the State. The State may, in its sole discretion and at Contractor's sole expense, require Contractor to engage the services of an independent, qualified, State-approved third party to conduct a security audit. Contractor shall provide the State with the results of such audit and evidence of Contractor's planned remediation in response to any negative findings.

E. Data Protection and Handling

Contractor shall ensure that all State Records and Work Product in the possession of Contractor or any Subcontractors are protected and handled in accordance with the requirements of this Contract, including any requirements set forth in Exhibits, at all times.

F. Safeguarding PII

If Contractor or any of its Subcontractors will or may receive PII under this Contract, Contractor shall provide for the security of the PII, in a manner and form acceptable to the

State, including, without limitation, State non-disclosure requirements, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, and audits. Contractor shall be a "Third-Party Service Provider" as defined in §24-73-103(1)(i), C.R.S. and shall maintain security procedures and practices consistent with §§24-73-101 *et seq*., C.R.S.

11. CONFLICTS OF INTEREST

A. Actual Conflicts of Interest

Contractor shall not engage in any business or activities or maintain any relationships that create a conflict of interest by conflicting in any way with the full performance of Contractor's obligations under this Contract. Such a conflict of interest arises when a Contractor's or Subcontractor's employee, officer, or agent: (i) offers or provides any tangible personal benefit to a State employee, a State employee's partner, or a member of a State employee's immediate family; or (ii) discusses, arranges for, or accepts financial or performance auditing work or non-auditing work not identified in this Contract with the Agency during the term of this Contract without the express written approval of the State.

B. Apparent Conflicts of Interest

Contractor acknowledges that with respect to this Contract even the appearance of a conflict of interest is harmful to the State's interests. Accordingly, absent the State's prior written approval, Contractor shall refrain from any practices, activities, or relationships that reasonably appear to conflict with Contractor's full performance of its obligations under this Contract. Contractor shall also provide written notice to the State, in accordance with **§17** of this Contact, and obtain the State's prior written approval, before entering into a contract or engagement with another State agency, department, or division that is subject to audit by the State.

C. Disclosure of Conflicts of Interest

If a conflict of interest or the appearance of a conflict of interest arises, or if Contractor is uncertain whether a conflict of interest or the appearance of a conflict of interest has arisen, Contractor shall submit to the State a disclosure statement that sets forth the relevant details for the State's consideration. Failure to promptly submit a disclosure statement or to follow the State's direction in regard to the actual or apparent conflict of interest is a breach of this Contract.

12. REPRESENTATIONS AND WARRANTIES

Each Party has relied on the representations and warranties of the other Party set forth below in entering into this Contract.

A. Qualifications, Standards, and Manner of Performance

Contractor represents and warrants that it is qualified and, if applicable, warrants that it is licensed in accordance with applicable laws and regulations, to perform the Work and Services and deliver the Work Product.

B. Legal Authority – Contractor Signatory

Contractor represents and warrants that it possesses the legal authority to enter into this Contract and that it has taken all actions required by its procedures, bylaws, and applicable laws to exercise that authority and to lawfully authorize its undersigned signatory to execute this Contract, or any part of this Contract, and to bind Contractor to its terms. If requested by the State, Contractor shall provide the State with proof of Contractor's authority to enter into this Contract within fifteen (15) days of receiving the request.

C. Licenses, Permits, and Other Authorizations

Contractor represents and warrants that as of the Effective Date it has, and that at all times during the term of this Contract it will have and maintain, at its sole expense, all licenses, certifications, approvals, insurance, permits, and other authorizations required by law to

perform its obligations under this Contract. Contractor warrants that it will maintain all necessary licenses, certifications, approvals, insurance, permits, and other authorizations required to properly perform its obligations under this Contract, without reimbursement by the State or any adjustment in Contract Funds. Additionally, all employees, agents, and Subcontractors of Contractor performing Services under this Contract shall hold all required licenses or certifications, if any, required to perform their responsibilities. Contractor, if a foreign corporation or other foreign entity transacting business in the State of Colorado, further warrants that it currently has obtained and will continue to maintain any applicable certificate of authority required to transact business in the State and that it has designated a registered agent in the State to accept service of process. Any revocation, withdrawal or non-renewal of licenses, certifications, approvals, insurance, permits, or other authorizations necessary for Contractor to properly perform the terms of this Contract is a material breach by Contractor and is grounds for termination of this Contract.

D. Contractor Independence

Contractor should be independent in performing the evaluation engagement. The State represents and warrants that it will not request or require Contractor to surrender Contractor's "independence" as that term is professionally understood and used.

E. Contractor Compliance with IRS Publication 1075

To the extent that Contractor receives, transmits, processes, and/or stores Federal Tax Information (FTI) on behalf of the State, Contractor will comply with IRS Publication 1075. Contractor and Contractor's employees with access to or who use FTI must meet the background investigation requirements set forth in IRS Publication 1075.

F. Disclaimer

Except for the representations and warranties expressly stated in this Contract, the Parties disclaim all representations and warranties, written or oral, express or implied.

13. INSURANCE

Contractor shall obtain and maintain, and shall ensure that each Subcontractor obtains and maintains, insurance policies issued by insurance companies approved by the State at all times during the term of this Contract as follows and in accordance with the following requirements:

A. Workers' Compensation

Workers' compensation insurance as required by state statute, and employers' liability insurance covering all Contractor or Subcontractor employees acting within the course and scope of their employment.

B. General Liability

Commercial general liability insurance covering premises operations, fire damage, independent contractors, products and completed operations, blanket contractual liability, personal injury, and advertising liability with minimum limits as follows:

i. $1,000,000 each occurrence;
ii. $1,000,000 general aggregate;
iii. $1,000,000 products and completed operations aggregate; and
iv. $50,000 any 1 fire.

C. Automobile Liability

Automobile liability insurance covering any auto (including owned, hired, and non-owned autos) with a minimum limit of $1,000,000 each accident combined single limit.

D. Protected Information

Liability insurance covering all losses of State Confidential Information, such as PII, PHI, PCI, Tax Information, and CJI, and claims based on alleged violations of privacy rights through improper use or disclosure of protected information with minimum limits as follows:

i. $1,000,000 each occurrence; and
ii. $2,000,000 general aggregate.

E. Professional Liability Insurance

Professional liability insurance covering any damages caused by an error, omission, or negligent act with minimum limits as follows:

i. $1,000,000 each occurrence; and

ii. $1,000,000 general aggregate.

F. Crime Insurance

Crime insurance including employee dishonesty coverage with minimum limits as follows:

i. $1,000,000 each occurrence; and

ii. $1,000,000 general aggregate.

G. Additional Insured

The State must be named as additional insured on all commercial general liability policies required of Contractor and Subcontractors.

H. Primacy of Coverage

Coverage required of Contractor and each Subcontractor must be primary over any insurance or self-insurance program carried by Contractor or the State.

I. Cancellation

The above insurance policies must include provisions preventing cancellation or non-renewal, except for cancellation based on non-payment of premiums, without at least thirty (30) days written prior notice to Contractor, and Contractor shall forward any such notice to the State in accordance with **§16** of this Contract within seven (7) days of Contractor's receipt of such notice.

J. Subrogation Waiver

All insurance policies secured or maintained by Contractor or its Subcontractors as required by this Contract must include clauses stating that each carrier waives all rights of recovery under subrogation or otherwise against Contractor, the State, and the State's agencies, institutions, organizations, officers, agents, employees, and volunteers.

K. Public Entities

If Contractor is a "public entity" within the meaning of the Colorado Governmental Immunity Act, §§24-10-101, *et seq.*, C.R.S. (the "GIA"), Contractor shall maintain, in lieu of the liability insurance requirements stated above, at all times during the term of this Contract such liability insurance, by commercial policy or self-insurance, as is necessary to meet its liabilities under the GIA. If a Subcontractor is a public entity within the meaning of the GIA, Contractor shall ensure that the Subcontractor maintain at all times during the terms of this Contract, in lieu of the liability insurance requirements stated above, such liability insurance, by commercial policy or self-insurance, as is necessary to meet the Subcontractor's obligations under the GIA.

L. Certificates

Contractor shall provide to the State certificates evidencing Contractor's insurance coverage required in this Contract within seven (7) Business Days following the Effective Date. Contractor shall provide to the State certificates evidencing Subcontractor insurance coverage required under this Contract within seven (7) Business Days following the Effective Date, except that, if Contractor's subcontract is not in effect as of the Effective Date, Contractor shall provide to the State certificates showing Subcontractor insurance coverage required under this Contract within seven (7) Business Days following Contractor's execution of the subcontract. No later than fifteen (15) days before the expiration date of Contractor's or any Subcontractor's coverage, Contractor shall deliver to the State certificates of insurance evidencing renewals of coverage. At any other time during the term of this Contract, upon request by the State, Contractor shall, within seven (7) Business Days following the request by the State, supply to the State evidence satisfactory to the State of compliance with the provisions of this **§13**.

14. DISPUTE RESOLUTION

Any dispute concerning the performance of this Contract that cannot be resolved by the designated Contract representatives shall be referred in writing to the State Auditor and the Contractor's managing partner or similar executive-level decision maker for resolution. The State Auditor and the Contractor's managing partner or similar executive-level decision maker shall informally discuss the dispute and attempt to resolve it. If the State Auditor and the Contractor's managing partner or similar executive-level decision maker are able to agree to a mutual resolution of the dispute, the resolution will be formalized in writing in accordance with this Contract. If either Party finds, at any time, that the attempted resolution of the dispute has failed, at which time each Party may pursue any and all remedies, including without limitation, those available under this Contract, at law or in equity.

15. BREACH OF CONTRACT

A. Defined

In addition to any breaches specified in other sections of this Contract, each of the following is a breach of this Contract:

i. Material Obligations

The failure of Contractor to perform, in whole or in part or in a timely or satisfactory manner, any of its material obligations under this Contract to the satisfaction of the State.

ii. Satisfactory Performance

A determination by the State, in its reasonable discretion, that satisfactory performance of Contractor's obligations under this Contract is substantially endangered.

iii. Bankruptcy

The institution of proceedings under any bankruptcy, insolvency, reorganization, or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property if the proceedings are not vacated or fully stayed within twenty (20) days after being instituted or occurring.

iv. Material Misrepresentation

Any statement, representation, or certification furnished by Contractor in connection with the RFP, Contractor's Proposal, Modifications to Contractor's Proposal, or this Contract that is false, deceptive, incorrect, or incomplete in any material respects.

v. Failure to Timely Deliver Reports

Failure by Contractor to complete and deliver the Evaluation Report or Work Product by the date specified in **§6(A)** of this Contract, unless Contractor can show that the delinquency resulted from causes beyond its control, such as failure of the Agency to provide, by the date specified in a written request from Contractor: requested documentation, records, or information; records that are auditable; or responses to Contractor's findings and recommendations. Contractor shall allow a reasonable amount of time for the Agency to provide the requested documentation, records, or information and responses.

vi. Debarment or Suspension

Debarment or suspension of Contractor under §24-109-105, C.R.S. at any time during the term of this Contract.

B. Notice and Cure Period

In the event of a breach, the aggrieved Party shall give written notice specifying the nature of the breach to the other Party in the manner provided in **§17** of this Contract. If a breach by Contractor is not cured within twenty (20) days of receipt of written notice, or, if a cure cannot be completed within twenty (20) days, the cure has not begun within twenty (20) days and been pursued with due diligence, the State may exercise any of the remedies set forth in **§16** of this Contract. Notwithstanding anything to the contrary in this Contract, the State, in its sole discretion, need not provide advance notice of a cure period and may

immediately terminate this Contract in whole or in part if reasonably necessary to preserve public safety or prevent immediate public crisis.

16. REMEDIES

If Contractor fails to cure a breach of this Contract in accordance with **§15(B)** of this Contract, the State may exercise any or all of the remedies available to it, including but not limited to the following remedies, in its sole discretion, concurrently or consecutively.

A. Termination for Breach

The State may terminate this Contract upon written notice to Contractor. Exercise by the State of this right is not be a breach of its obligations under this Contract.

B. Liquidated Damages

If Contractor fails to complete and deliver the Evaluation Report by the date specified in **§6(A)** of this Contract, Contractor shall pay liquidated damages to the State of $100 per day for each day delinquent. To the extent that Contractor's failure is excused under **§15(A)(v)** of this Contract, Contractor is not required to pay the liquidated damages. The Parties agree that the damages from Contractor's failure to timely deliver the Evaluation Report are difficult to estimate, and that the amount of liquidated damages specified in this **§16(B)** represents a reasonable estimation of damages that the State will incur due to late performance. Assessment of liquidated damages is not exclusive and does not limit the remedies available to the State, at law or in equity, for other breaches of this Contract by Contractor.

C. Withold Payment

The State may withhold payment to Contractor until corrections in Contractor's performance are satisfactorily made and completed.

D. Deny Payment

The State may deny payment for obligations not performed if, due to Contractor's actions or inactions, the obligation cannot be performed or, if performed, would be of no value to the State. Any denial of payment must be reasonably related to the value to the State of the obligations not performed.

E. Noncompliance with Federal Regulations

Contractor is liable for any and all penalties applied by the federal government due to noncompliance with federal regualtions by Contractor, a Subcontractor, or any of Contractor's employees.

17. NOTICES AND REPRESENTATIVES

Each individual identified below is the principal representative of the designating Party. All notices required or permitted to be given to a Party under this Contract must be in writing and must be delivered: (i) by hand with receipt required; (ii) by certified or registered mail to the Party's principal representative at the address set forth below; or (iii) as an email with read recept requested to the principal representative at the email address, if any, set forth below. If a Party delivers notice to the other Party by email and the email is undeliverable, then, unless the delivering Pary is provided with an alternative email address, the Party shall deliver the notice by hand with receipt required or by certified or registered mail to the other Party's principal representative at the address set forth below. Either Party may change its principal representative or principal representative contact information, or may designate specific other individuals to receive certain types of notices in addition to or in lieu of a principal representative by notice submitted in accordance with this **§17** without making a formal amendment to this Contract. Unless otherwise provided in this Contract, notices are effective upon delivery in accordance with this **§17**.

A. State:

Kerri Hunter,

Deputy State Auditor
Office of the State Auditor
1525 Sherman St., 7th Floor
Denver, Colorado 80203-1700
kerri.hunter@state.co.us

B. Contractor:

Name, Title
Company Name
Address
City, State Zip
Email

C. Media

The State is the official spokesperson to the news media pertaining to the Work, Services, and Work Product. Contractor shall forward immediately to the State any inquiries from the news media pertaining to the Work, Services, or Work Product.

18. RIGHTS IN WORKPAPERS

The workpapers developed by Contractor during the performance of the Services are the exclusive property of Contractor. The State has the right to copy the workpapers. Except as provided in **§§9B** and **10** of this Contract, Contractor shall not provide the workpapers to third parties or permit third parties to review, access, or use the workpapers for public inspection unless, and only to the extent that, the Legislative Audit Committee has specifically approved disclosure of the workpapers in accordance with §2-3-103(3), C.R.S., and the State has given Contractor prior written consent to disclose the workpapers. Contractor shall forward immediately to the State any requests for workpapers that Contractor receives pursuant to CORA.

19. STATEWIDE CONTRACT MANAGEMENT SYSTEM - EXEMPTION

Because this contract is a legislative department contract, it is not included within the State's contract management system, which includes only personal services contracts that are entered into by a "governmental body," as defined in section 24-101-301, C.R.S. That definition of "governmental body" does not include the legislative department or its agencies.

20. GENERAL PROVISIONS

A. Assignment and Subcontracts

Contractor's rights and obligations under this Contract are personal and may not be transferred, assigned, or subcontracted without the prior written consent of the State. Any attempt at assignment, transfer, or subcontracting without such prior written consent is void. Any assignment, transfer, or subcontracting of Contractor's rights or obligations under this Contract that is approved by the State is subject to the provisions of this Contract. Upon the request of the State, Contractor shall provide to the State a copy of any subcontract entered into by Contractor in connection with this Contract. Contractor is solely responsible for all aspects of subcontracting arrangements and performance, and any subcontract entered into by Contractor in connection with this Contract must comply with all applicable federal and state laws and regulations and provide that it is subject to all provisions of this Contract and governed by the laws of the State.

B. Binding Effect

Except as otherwise provided in **§20(A)** of this Contract, all provisions of this Contract, including the benefits and burdens, extend to and bind the Parties' respective successors and assigns.

C. Captions and References

The captions and headings in this Contract are for convenience of reference only, and shall not be used to interpret, define, or limit its provisions. Unless the context clearly otherwise requires, all references in this Contract to sections (whether spelled out or using the § symbol), subsections, or Exhibits refer to sections, subsections, or Exhibits contained in this Contract or incorporated by reference into this Contract.

D. Counterparts

This Contract may be executed in multiple identical original counterparts, each of which is an original, but all of which, taken together, constitute one and the same agreement.

E. Entire Understanding

This Contract represents the complete integration of all understandings between the Parties related to the Work, Services, and Work Product and all prior representations and understandings related to the Work, Services, and Work Product, whether oral or written are merged into this Contract. Prior or contemporaneous additions, deletions, or other changes to this Contract do not have any force or affect whatsoever, unless embodied in this Contract.

F. Digital Signatures

If any signatory signs this agreement using a digital signature, any agreement or consent to use digital signatures within the electronic system through which that signatory signed is incorporated into this Contract by reference.

G. Modification

Except as otherwise provided in this Contract, any modification of this Contract is only effecitve if agreed to in a formal written amendment to this Contract that is properly executed and approved in accordance with applicable State law.

H. Statutes, Rules, Regulations, and Other Authority

Unless otherwise specifically provided, any reference in this Contract to a federal or state statute, rule, or regulation or to any other source of legal or policy authority refers to the current version of the statute, rule, regulation, or other authority including any amendments or changes to the authority made after the Effective Date.

I. Order of Precedence

If a conflict or inconsistency arises between any provision contained in the main body of this Contract and any Exhibit, the conflict or inconsistency must be resolved by reference to the documents in the following order of priority:

i. Colorado Legislative Branch Special Provisions;

ii. The remaining provisions of the main body of this Contract; and

iii. The Exhibits

J. External Terms and Conditions

Notwithstanding anything to the contrary in this Contract, the State is not subject to any provision included in any terms, conditions, or agreements appearing on Contractor's or a Subcontractor's website or any provision incorporated into any click-through or online agreements related to the Work unless this Contract specifically references that provision.

K. Severability

The invalidity or unenforseability of any provision of this Contract does not affect the validity of or enforceability of any other provision of this Contract, which remains in full force and effect, so long as the Parties can continue to perform their obligations under this Contract in accordance with the intent of the Parties.

L. Survival of Certain Contract Terms

Any provision of this Contract that imposes an obligation on a Party that begins after or continues after the termination or expiration of this Contract survives the termination or expiration of this Contract and is enforceable by the other Party.

M. Taxes

The State is exempt from federal excise taxes under I.R.C. Chapter 32 (26 U.S.C. Subtitle D, Ch. 32) (Federal Excise Tax Exemption Certificate Registry No. 84-730123K) and from all State and local government sales and use taxes under §§39-26-704(1), and 29-2-105(1)(d)(I), C.R.S. (Colorado Sales Tax Exemption Identification Number 98-20565). The State is not liable for the payment of excise, sales, or use taxes, regardless of whether any political subdivision of the State imposes such taxes on Contractor. Contractor is solely responsible for any exemptions from the collection of excise, sales, or use taxes that Contractor may wish to have in place in connection with this Contract.

N. Third Party Beneficiaries

Except for a person who assumes Contractor's rights and obligations under this Contract as a successor or assign in accordance with **§§20(A)** and **20(B)** of this Contract, this Contract does not and is not intended to confer any rights, obligations, or remedies upon any person or entity other than the Parties. Enforcement of this Contract and all rights and obligations under this Contract are reserved solely to the Parties. Any services or benefits that third parties receive as a result of this Contract are incidental to the Contract and do not create any rights for the third parties.

O. Waiver

A Party's failure or delay in exercising any right, power, or privilege under this Contract, whether explicitly or by lack of enforcement, does not operate as a waiver of the right, power, or privilege, and a single or parial exercise of any right, power, or privilege does not preclude any other or further exercise of the right, power, or privilege.

P. CORA Disclosure

This Contract is a public record that, to the extent not prohibited by federal law, is subject to public release through CORA.

Q. Standard and Manner of Performance

Contractor shall perform its obligations under this Contract in accordance with the highest standards of care, skill, and diligence in Contractor's industry, trade, or profession.

R. Indemnification

i. General Indemnification

Contractor shall indemnify, save, and hold harmless the State and the State's employees, agents, and assignees ("Indemnified Parties"), against any and all costs, expenses, claims, damages, liabilities, court awards, attorney's fees and costs, and other amounts claimed by third parties and incurred by any of the Indemnified Parties to the extent caused by any negligence, intentional, or deliberate act or omission by Contractor or Contractor's employees, agents, Subcontractors, or assignees in connection with this Contract.

ii. Confidential Information Indemnification

Disclosure or use of State Confidential Information by Contractor in violation of this Contract may be cause for legal action by third parties against Contractor, the State, or their respective agents. Contractor shall indemnify, save, and hold harmless the Indemnified Parties against any and all costs, expenses, claims, damages, liabilities, court awards, attorneys' fees and costs, and other amounts, claimed by third parties and incurred by the State to the extent caused by any act or omission by Contractor or Contractor's employees, agents, assigns, or Subcontractors that violates this Contract.

iii. Intellectual Property Indemnification

Contractor shall indemnify, save, and hold harmless the Indemnified Parties against any and all costs, expenses, claims, damages, liabilities, court awards, and other amounts, including attorneys' fees and costs, incurred by the Indemnified Parties in relation to any

claim that any Work infringes a patent, copyright, trademark, trade secret, or any other intellectual property right.

S. Limitation of Contractor Liability

Any liability of Contractor and its personnel to the State for any breach of this contract or act or omission that directly damages the State is limited to the amount of the fee to be paid by the State to Contractor under this Contract. This limitation does not apply to any requirement of this Contract that Contractor indemnify the State for liabilities of the State to any third party that result from any negligent, intentional, or deliberate acts or omissions of Contractor.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

21. COLORADO LEGISLATIVE DEPARTMENT SPECIAL PROVISIONS

These Special Provisions apply to all legislative department contracts except where noted in italics.

A. FUND AVAILABILITY. §24-30-202 (5.5), C.R.S.

Financial obligations of the State payable after the current State Fiscal Year are contingent upon funds for that purpose being appropriated, budgeted, and otherwise made available.

B. GOVERNMENTAL IMMUNITY.

Liability for claims for injuries to persons or property arising from the negligence of the State, its departments, boards, commissions, committees, bureaus, offices, employees, and officials is controlled and limited by the provisions of the Colorado Governmental Immunity Act, §24-10-101, et seq., C.R.S., the Federal Tort Claims Act, 28 U.S.C. Pt. VI, Ch. 171, and 28 U.S.C. §1346(b), and the State's risk management statutes, §24-30-1501, et seq., C.R.S. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions contained in these statutes.

C. INDEPENDENT CONTRACTOR.

Contractor shall perform its duties under this Contract as an independent contractor and not as an employee. Neither Contractor nor any agent or employee of Contractor shall be deemed to be an agent or employee of the State. Contractor shall not have authorization, express or implied, to bind the State to any agreement, liability, or understanding, except as expressly set forth in this Contract. Contractor and its employees and agents are not entitled to unemployment insurance or workers' compensation benefits through the State, and the State shall not pay for or otherwise provide such coverage for Contractor or any of its employees or agents. Contractor shall pay when due all applicable employment taxes, income taxes, and local head taxes incurred pursuant to this Contract. Contractor shall: **(i)** provide and keep in force workers' compensation and unemployment compensation insurance in the amounts required by law, **(ii)** provide proof thereof when requested by the State, and **(iii)** be solely responsible for its acts and the acts of its employees and agents.

D. COMPLIANCE WITH LAW.

Contractor shall comply with all applicable federal and State laws, rules, and regulations in effect or hereafter established, including, without limitation, laws applicable to discrimination and unfair employment practices.

E. CHOICE OF LAW, JURISDICTION, AND VENUE.

Colorado law, and rules and regulations issued pursuant to Colorado law, apply to the interpretation, execution, and enforcement of this Contract. Any provision included in or incorporated into this Contract by reference that conflicts with said law, rules, or regulations is void. All suits or actions related to this Contract must be filed and proceedings held in the State of Colorado, and exclusive venue is in the City and County of Denver.

F. PROHIBITED TERMS.

Any term included in this Contract that requires the State to indemnify or hold Contractor harmless; requires the State to agree to binding arbitration; limits Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or conflicts with this provision in any way is void. Nothing in this Contract shall be construed as a waiver of any provision of §24-106-109, C.R.S. Any term included in this Contract that limits Contractor's liability that is not void under this section applies only in excess of any insurance to be maintained under this Contract, and no insurance policy shall be interpreted as being subject to any limitations of liability of this Contract.

G. SOFTWARE PIRACY PROHIBITION.

State or other public funds payable under this Contract shall not be used for the acquisition, operation, or maintenance of computer software in violation of federal copyright laws or applicable licensing restrictions. Contractor hereby certifies and warrants that, during the term of this Contract and any extensions, Contractor has and shall maintain in place appropriate systems and controls to prevent such improper use of public funds. If the State determines that Contractor is in violation of this provision, the State may exercise any remedy available at law, in equity, or under this Contract, including, without limitation, immediate termination of this Contract and any remedy consistent with federal copyright laws or applicable licensing restrictions.

H. EMPLOYEE FINANCIAL INTEREST/CONFLICT OF INTEREST. §§24-18-201 and 24-50-507, C.R.S.

The signatories aver that to their knowledge, no employee of the State has any personal or beneficial interest whatsoever in the service or property described in this Contract. Contractor has no interest and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of Contractor's services, and Contractor shall not employ any person having such known interests.

I. VENDOR OFFSET AND ERRONEOUS PAYMENTS. §§24-30-202 (1) and 24-30-202.4, C.R.S.

[Not applicable to intergovernmental agreements] Subject to §24-30-202.4(3.5), C.R.S., the State Controller may withhold payment under the State's vendor offset intercept system for debts owed to State agencies for: **(i)** unpaid child support debts or child support arrearages; **(ii)** unpaid balances of tax, accrued interest, or other charges specified in §39-21-101, et seq., C.R.S.; **(iii)** unpaid loans due to the Student Loan Division of the Department of Higher Education; **(iv)** amounts required to be paid to the Unemployment Compensation Fund; and **(v)** other unpaid debts owing to the State as a result of final agency determination or judicial action. The State may also recover, at the State's discretion, payments made to Contractor in error for any reason, including, but not limited to, overpayments, improper payments, and any other unexpended or excess funds received by Contractor, by deduction from subsequent payments under this Contract, by deduction from any payment due under any other contracts, grants or agreements between the State and Contractor, or by any other appropriate method for collecting debts owed to the State.

J. PUBLIC CONTRACTS FOR SERVICES. §8-17.5-101 *et seq.*, C.R.S.

[Not applicable to agreements relating to the offer, issuance, or sale of securities, investment advisory services or fund management services, sponsored projects, intergovernmental agreements, or information technology services or products and services] Contractor certifies, warrants, and agrees that it does not knowingly employ or contract with an illegal alien who will perform work under this Contract and will confirm the employment eligibility of all employees who are newly hired for employment in the United States to perform work under this Contract through participation in the E-Verify Program or the State verification program established pursuant to §8-17.5-102(5)(c), C.R.S. Contractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract or enter into a contract with a Subcontractor that fails to certify to Contractor that the Subcontractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract. Contractor: **(i)** shall not use the E-Verify Program or the program procedures of the Colorado Department of Labor and Employment ("Department Program") to undertake pre-employment screening of job applicants while this Contract is being performed; **(ii)** shall notify the Subcontractor and the contracting State agency within 3 days if Contractor has actual knowledge that a Subcontractor is employing or contracting with an illegal alien for work under this Contract; **(iii)** shall terminate the subcontract if a Subcontractor does not stop employing or contracting with

the illegal alien within 3 days of receiving the notice; and **(iv)** shall comply with reasonable requests made in the course of an investigation, undertaken pursuant to §8-17.5-102(5), C.R.S., by the Colorado Department of Labor and Employment. If Contractor participates in the Department Program, Contractor shall deliver to the contracting State agency a written, notarized affirmation affirming that Contractor has examined the legal work status of such employee, and shall comply with all of the other requirements of the Department Program. If Contractor fails to comply with any requirement of this provision or §8-17.5-101, et seq., C.R.S., the contracting State agency may terminate this Contract for breach and, if so terminated, Contractor shall be liable for damages.

K. PUBLIC CONTRACTS WITH NATURAL PERSONS. §§24-76.5-101, *et seq.*, C.R.S. Contractor, if a natural person 18 years of age or older, hereby swears and affirms under penalty of perjury that he or she: **(i)** is a citizen or otherwise lawfully present in the United States pursuant to federal law; **(ii)** shall comply with the provisions of §24-76.5-101, *et seq.* C.R.S.; and **(iii)** has produced one form of identification required by §24-76.5-103, C.R.S., prior to the Effective Date of this Contract.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

22.SIGNATURE PAGE
Contract Routing Number 20XX-XX

THE PARTIES HERETO HAVE EXECUTED THIS CONTRACT

Each person signing this Contract represents and warrants that the signer is duly authorized to execute this Contract and to bind the Party authorizing such signature.

CONTRACTOR

[INSERT NAME OF CONTRACTOR]

By:
Title:

_____
Signature

Date: _____

STATE OF COLORADO
Colorado Office of the State Auditor
Dianne E. Ray, State Auditor

_____
By: Dianne E. Ray, State Auditor

Signatory avers that Contractor has not begun performance or that a Statutory Violation waiver has been requested

Date: _____

_____
Legislative Audit Committee Chair

LEGAL REVIEW
Office of Legislative Legal Services
Sharon L. Eubanks, Director

By:_____
Jason A. Gelender, Managing Senior Attorney (designee of Sharon L. Eubanks, Director)

Date: _____

23. EXHIBIT A – STATEMENT OF WORK

1. GENERAL DESCRIPTION

Contractor shall conduct a performance evaluation of the Agency in a manner consistent with the terms and conditions of the Contract and its Exhibits.

2. CONTRACTOR'S OBLIGATIONS

The Work to be performed by Contractor includes the following:

A. Scope

Contractor's evaluation of the Agency must include the following:

1. [**ADD** detailed description of work to be completed.]
2. As it performs the Work, Contractor shall maintain an awareness of any areas beyond the scope of the Services in which the Agency may not be carrying out the Agency's programs in an effective and efficient manner. Contractor shall discuss any such areas with the State to determine whether the State desires Contractor to expand the scope of the Services of this Contract. The cost of such additional Services are not included within the scope of this Contract, and any additional Services shall be subject to negotiation and set forth in a separate agreement among Contractor, the State Auditor, and the Legislative Audit Committee.

B. Review by State

During the performance of Services under this Contract and prior to completion of the Work by the date specified in **§6(A)** of this Contract, the State has access to and the right to review Contractor's Work and Work Product, whether in draft or final form, for acceptability and to provide guidance, direction, and feedback and suggest revisions. Contractor may not submit written findings or the Evaluation Report, whether in draft or final form, to the Agency until they are deemed acceptable and approved by the State.

C. Availability

Contractor, upon the request of the State, shall furnish copies of Contractor's work programs developed pursuant to this Contract and make all other workpapers available to the State for review or use in future audits or evaluations, at no additional charge to the State.

D. Reports

Contractor shall prepare and deliver the Evaluation Report to the State no later than [Insert Date], unless the State has approved an extension of time. If Contractor becomes aware that the due date for the Evaluation Report cannot be met, Contractor shall notify the State in writing of the reasons for the delay and identify a specific date when the Evaluation Report will be delivered. For a separately issued Evaluation Report, Contractor shall deliver to the State up to 100 copies of the bound report as determined by the State at the time of report finalization. Acceptable binding formats for the Evaluation Report are limited to spiral, comb, or glued bindings; 3-ring bindings are not acceptable. Contractor shall also deliver to the State an electronic copy of the Evaluation Report in unprotected Adobe PDF format or any other format prescribed by the State.

E. Oral Presentations

Contractor shall make an oral presentation of the Evaluation Report to the Legislative Audit Committee and, if applicable and upon notification by the State, one other legislative committee.

F. Entrance/Exit Conferences

The State shall participate in all entrance and exit conferences between the Agency and Contractor, as well as other critical meetings, such as those dealing with findings.

G. Fraud

If Contractor becomes aware of fraud or indications of fraud affecting the Agency, Contractor shall notify the State immediately.

3. PERSONNEL

A. Contract Monitor

Contractor's performance under this Contract shall be monitored by [name of contract monitor], an employee or agent of the State, who is hereby designated as the Contract Monitor. The Contract Monitor shall review Contractor's Work and Work Product, attend key meetings (*e.g.,* entrance and exit conferences), and act as a liaison between the OSA, Contractor, and the Agency. With the exception of contract monitoring activities, and unless otherwise noted in this Contract, the State is not required to provide any additional staff time in connection with the Services provided or Work performed.

B. Other Key Personnel

The key personnel identified by Contractor in the Contractor's Proposal are deemed to be essential to the Work being performed under the Contract.

C. Replacement

Contractor shall immediately notify the State if any key personnel cease to be employed by Contractor. Before diverting any key personnel to other programs, Contractor shall give the State fifteen (15) days advance notice and shall submit to the State justification, including proposed personnel substitutions, in sufficient detail to permit evaluation of the impact on the Contractor's performance of the Work. Contractor shall not divert any key personnel without the prior written consent of the State, which the State shall not unreasonably withhold. Contractor shall replace any key personnel with personnel of substantially equal or greater ability and qualifications to perform the Work.

4. ACCEPTANCE CRITERIA

If the State determines that the Work or Work Product is unacceptable (either before or after a draft or a final Evaluation Report is issued) due to Contractor's failure to satisfy any requirements included in this Contract, the State, at the State's direction, may require Contractor to re-perform the Work at its own expense and submit a revised Work Product. The State's right to reject Contractor's draft or final Evaluation Report because of the failure to comply and Contractor's obligation to re-perform or revise extend throughout the term of this Contract and continue for one (1) full year after the termination of this Contract.

5. PAYMENTS

Payments shall be made in accordance with **Exhibit F** and any other applicable provisions of this Contract.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

24. EXHIBIT B – REQUEST FOR PROPOSAL

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

25. EXHIBIT C – MODIFICATIONS TO CONTRACTOR'S PROPOSAL

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

26. EXHIBIT D –CONTRACTOR'S PROPOSAL

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

27. EXHIBIT E - INFORMATION SECURITY POLICY FOR CONTRACTORS

Applicability

This policy applies to all OSA Contractors at all locations who are conducting audits, evaluations, or other professional services on behalf of the OSA using State of Colorado information or any information, electronic or otherwise, obtained, utilized, or generated by an OSA Contractor while performing work on behalf of the OSA.

Definitions

Confidential information assets – are defined in paragraph 5. below.

OSA Contractor(s) or Contractor(s) – any business, company, corporation, partnership, or individual conducting business on behalf of or in cooperation with the OSA, whether via contract, purchase order, or other purchasing agreement. OSA Contractors include Subcontractors and their employees.

Protected information assets - are defined in paragraph 4. below.

State of Colorado information, information or audit information – any information, whether in electronic or hard copy form, obtained, utilized, or generated by an OSA Contractor while performing work on behalf of the OSA.

State Auditor Authority and Responsibility

The State Auditor's authority and responsibility for accessing and handling confidential information is set forth in the Colorado Revised Statutes. Section 2-3-107(2)(a), C.R.S., provides that the State Auditor or his or her designated representative "shall have access at all times …. to all of the books, accounts, reports, vouchers, or other records or information in any department, institution, or agency, including records or information required to be kept confidential or exempt from public disclosure upon subpoena, search warrant, discovery proceedings, or otherwise." Additionally, Section 2-3-103(3), C.R.S., provides that "work papers of the office of the State Auditor shall be open to public inspection only upon approval of the majority of the members of the audit committee" and that "work papers that have not been specifically approved for disclosure by a majority vote of the committee shall remain confidential." Finally, Sections 2-3-103.7 and 2-3-107(2)(b), C.R.S., prescribe penalties for willful or unlawful release of confidential information and prohibit the release of information required to be kept confidential pursuant to any law. The volume and availability of confidential information in electronic and hardcopy format, along with the risk to the OSA should confidential information be inadvertently released or breached, heightens the need for rigorous procedures governing the receipt, storage, and destruction of confidential data.

Policy Compliance

1. All OSA Contractors and their personnel who are performing the Work are required to understand and abide by this policy.

2. By signing an OSA contract or purchase order, an OSA Contractor agrees to abide by this policy and require its personnel performing the Work, including Subcontractors and their employees, to understand and abide by this policy.

Data Classification

3. Any State information asset whether in hardcopy or electronic form (e.g., data, databases, reports, communications, manuals, documentation for systems, procedures, and plans) that is used in the course of an audit on behalf of the OSA is considered either "Protected" or "Confidential," unless expressly stated otherwise in writing by the State Auditor.

4. "Protected information assets" are defined as information that: (i) is required by federal, state, or local laws and statutes to be protected; or (ii) would, in the event of a breach of confidentiality, loss of integrity, or lack of availability, seriously and adversely impact the OSA or the State, up to and including physical harm to individuals, or cause significant hardship to the OSA, the State, or commercial entities that have entrusted the information to the OSA.

5. All OSA Contractor audit information not categorized as "Protected" are automatically classified as "Confidential."

Use and Protection of Information Assets

6. Contractors must take reasonable and prudent measures to protect all OSA audit information and the systems that process, store, and transmit such information from unauthorized disclosure and modification regardless of where the OSA audit information and the systems are located.

7. All State information systems (e.g., networks, intranets, internet connections, telephones, fax, etc.) are the property of the State and are for State business use only. Contractor shall not use State information systems to knowingly access, store, or distribute offensive material, such as pornography. Contractors may not use State of Colorado systems to knowingly compromise other systems, networks or safeguards unless the OSA specifically authorizes them to do so in order to test the security of such systems, networks, or safeguards for legitimate State purposes.

8. Any unauthorized attempt to access information that is outside Contractor's "need-to-know" for his/her operational purposes is prohibited.

9. Contractors must encrypt all "Protected" and "Confidential" information when stored on portable computers or removable media (e.g., laptops, external hard drives, CDs, USB drives.)

10. Contractors must, at all times, physically secure portable computers used in storing and processing audit information on behalf of the OSA through the use of cable locks or other security measures or, when physically securing a portable computer at a work site is not feasible, use encrypted devices or other security measures to ensure that theft of a portable computer does not result in the loss or disclosure of State Confidential Information or Work Product.

11. Contractors shall not leave any portable computers, removable media (e.g., laptops, external hard drives, CDs, USB drives), or hard copy information containing "Protected" and "Confidential" information unattended, such as in vehicles or in checked airport luggage.

Viruses and Malicious Code

12. Contractors must effectively deploy personal firewall security and up-to-date malicious code/virus protection software for all systems and devices used to access audit information or in carrying out official OSA business.

Telecommunications Security and Information Transmission

13. Contractors are responsible for being aware of and protecting against current and potential telecommunications (e.g., telephones, voice mail, mobile phones, conference calls, instant messaging, and facsimile machines) security risks in their given environment.

14. Contractors are prohibited from connecting to any state networks in connection with the Services hereunder without prior authorization from the OSA and the information security officer of the Audited Agency. In the case of executive branch agencies, Contractors should submit a request with their agency liaison to obtain permission through the Governor's Office of Information Technology access management team.

15. Contractors shall make every effort to ensure that all State of Colorado information is protected from inadvertent disclosure when being sent over the Internet or other non-State of Colorado networks.

16. Contractors shall not connect portable computers containing "Protected" or "Confidential" data to any public WiFi networks (e.g., internet cafes) without adequately protecting such information through the use of hard drive encryption and the use of an encrypted VPN tunnel.

17. Contractors must always consider information sensitivity and transmission security issues when selecting a transmission medium. "Protected" and "Confidential" data must only be transported or transmitted over a public network when protected by encryption.

18. When data is stored on electronic media or a mobile computing device, the data must be encrypted at all times during physical transport.

19. Transmission of Protected or Confidential data over a public network by unencrypted email is prohibited.

Information Storage and Disposal

20. Media or hard copy documents containing Protected or Confidential information are to be appropriately labeled as such and protected in accordance with this **Exhibit E**.

21. Contractors must maintain physical media security by using locking filing cabinets or drawers and locking them when left unattended. Media security may also be achieved by locking the door of a private office.

22. Personal computers, laptops, USB drives, mobile phones, personal digital assistants (PDAs), and other devices and media containing State of Colorado information must be secured by their users from loss, theft, and unauthorized use.

23. Contractors shall not leave unattended any device containing State of Colorado information unless a password-engaged screensaver is used. The screen saver must engage after no more than 2 minutes of inactivity unless Contractor has a policy that requires its employees and its Subcontractors' employees to manually lock the device when leaving it unattended.

24. Contractors must ensure that once portable storage devices (e.g., external hard drives, CDs, USB drives) that will be leaving their effective control or are at the end of their useful lives, are cleaned and sanitized (i.e., cleared, purged, and destroyed) of all Protected or Confidential data in conformance with NIST

Special Publication 800-88 and/or other standard procedures and requirements set by the U.S. Department of Defense, such as DoD 5220.22-M.

25. Hard copy documents containing Protected or Confidential information must be shredded prior to disposal.

26. Data storage devices (e.g., CDs, DVDs, and floppy disks) containing Protected data must be physically destroyed at the end of the audit. For thumb drives and portable hard drives, Contractor must either use an electronic shredding program to destroy the data or destroy the device at the end of the audit. A record of disposal is to be maintained in the workpapers by the Contractors. A record of disposal must contain the name of the individual disposing of the data, the method used to dispose of the data, identifying qualities of the data (such as the serial number of the media on which it was stored, if applicable), and the date of disposal.

Incident Reporting

27. All suspected loss or compromise of OSA audit information as a result of the loss of a desktop, portable, or mobile computing device or removable storage device by any means (e.g., theft, loss) used to store State of Colorado data shall be reported to the OSA Contract Manager within 24 hours of discovery.

28. In the event of the suspected loss or compromise of OSA audit information under control of Contractor, Contractor is responsible for working with the State Auditor and the Audited Agency with respect to recovery and remediation. Contractor is also responsible for working with the OSA and the Audited Agency to notify all Colorado residents and other affected parties whose sensitive data may have been compromised as a result of the breach. Contractor will bear all reasonable associated costs.

Personnel Security

29. Contractor is responsible for performing background checks consistent with Contractor's standard employment practices for Contractor personnel completing work on behalf of the OSA.

Policy Enforcement

30. If Contractor is deemed to be in noncompliance of this policy by the State Auditor, the State Auditor may unilaterally terminate the Contract.

31. Upon request by the State Auditor, Contractor agrees that it shall make available qualified individuals and a member of senior management responsible for security and data protection for the purpose of discussing information technology controls, including those policies, procedures, and controls relevant to the provision of services and security obligations under this Contract.

28. EXHIBIT F - COMPENSATION AND PROCEDURES FOR BILLING

1. Contractor shall submit all invoices for services to the State. Payment will be made from the State Auditor's appropriation. Contractor shall not request payment from the Agency.

2. Contractor may render monthly interim bills to the State until completion of the Work, provided that the aggregate amount of all bills shall not exceed the maximum compensation set forth in **§3** of this **Exhibit F**. The interim bills shall be promptly paid by the State except that the State reserves the right to withhold 10 percent of the total Contract amount until delivery and acceptance of the Evaluation Report. Release of the Evaluation Report by the Legislative Audit Committee constitutes acceptance of the Evaluation Report.

3. Total maximum compensation for the Work is $XX,XXX.XX, with the estimated funding split between State Fiscal Years expected to be:

	Total	Paid From State's Budget Period	
		20XX-20XX	20XX-20XX
Contractor	$XX,XXX.XX	$XX,XXX.XX	$XX,XXX.XX
Total Fee	**$XX,XXX.XX**	**$XX,XXX.XX**	**$XX,XXX.XX**

29. EXHIBIT G - DEVELOPING AND PRESENTING FINDINGS

Title of Finding

Provide brief background information about the program in one or two paragraphs. Do not include criteria, condition, cause, or effect in this background section.

What work was performed and what was the purpose?

Briefly describe the testwork that was performed using bullets and/or one to two paragraphs. (i.e., describe the data and documents reviewed, individuals interviewed, and the sample selected and sample methodology).

Describe the purpose of the work in one sentence. (*i.e.,* "The purpose of the work was to XXXX.")

How were the results of the work measured? *(Criteria)*

The criteria are the standards against which the condition is measured. They are standards used to evaluate a particular event or process and describe "what should be." Some examples of criteria include:

- Colorado Constitution
- Colorado Revised Statutes
- Colorado state agency rules and regulations
- federal laws and regulations
- State Fiscal Rules and Fiscal Procedures Manual
- Generally Accepted Accounting Principles
- program-specific written policies and procedures
- program-specific written goals and objectives
- good business practices
- unwritten policies, procedures, goals, and objectives as explained by the Agency's personnel

If the criteria are not already set forth in writing, it may be necessary to find information to serve as evidence of criteria. When common sense or expert opinion is used as criteria, the development of the finding must be logical and convincing to the reader, who may not possess the same level of expertise. This is also important because such criteria are less authoritative than other types of criteria.

This section should briefly describe the criteria of the finding. Strive to provide the essential information in one or two short paragraphs, bullets, or in a table.

What problem did the work identify? *(Condition)*

The first step in developing a finding is to identify the statement of condition. This occurs during the "fact-finding" process when the evaluator compares "what is" with "what should be." When there is a difference between "what is happening" with "what should be happening," the first element (condition) of a finding is identified. The condition should be a factual statement of what was found and be free of value judgments.

This section should describe the overall problem (the condition of the finding) in one or two sentences. Then provide specific examples that support the condition (*e.g.,* exceptions identified during the test work). Use bullets and tables to describe the types of exceptions identified.

Why did the problem occur? *(Cause)*

The cause is the element of the finding which explains why the "condition" exists. The cause represents what must be corrected to prevent the recurrence of the existing condition. As such, evaluators must correctly identify the cause before a proper course of action can be devised. Developing the cause frequently requires a fairly extensive analysis of the problem. Often, there are multiple factors causing the problem. The human behavior aspect, which increases the difficulty in identifying the proper cause, is always present. Nevertheless, evaluators should make a reasonable effort to determine as closely as possible the real cause of the problem. Examples of cause include:

- negligence
- inadequate resources
- inadequate training
- poor communication
- inadequate guidelines or standards
- absence of good management techniques
- failure to follow established policies and procedures

This section should describe the cause of the finding in one or two paragraphs or in bullets that correspond to the bullets used in the condition section above.

Why does this problem matter? *(Effect)*

The effect represents the end result of the activity being measured. It is the impact of the difference between the statement of condition and the criteria. The attention given to a finding depends largely upon its significance, and significance is judged by effect. What is the result if nothing is done about the problem identified? Evaluators frequently use materiality to measure the potential significance of findings. The effect of an adverse finding is what motivates management to take needed action to correct the condition. When the effect is insignificant, the evaluator should consider eliminating the finding from the report or grouping it with other minor findings. Some examples of effect include:

- violation of law or regulation
- noncompliance with legislative intent
- loss of potential income

- program goals and objectives not being met
- increased costs
- poor service quality
- inefficient service delivery
- increased risk of fraud and abuse
- reduced effectiveness

When determining the effect of a finding, evaluators should look at outcomes such as impacts on citizens, services, or public safety. In addition, the fiscal impact of the finding (*e.g.,* increase or decrease in revenue or costs) should be quantified where possible. The estimated fiscal impact should be discussed with the Agency and reported as an estimate (*e.g.,* we estimate this change will eliminate one administrative support position with an estimated annual cost of $26,000).

This section should describe the effect of the finding in one or two paragraphs or bullets. Quantify the effect to the extent possible.

Recommendation No. X:

The recommendation is the action believed necessary to correct the adverse situation. Generally, each finding will result in one or more recommendations. The following are guidelines for developing recommendations:

- Write recommendations that address or solve the "cause" of the problem.
- Write recommendations as realistically and specifically as possible so they are more likely to be understood by and prove useful to the Agency.
- Present recommendations in a constructive tone and emphasize improvement rather than criticism of past activities. Evaluators should keep in mind that their objective is to motivate the Agency to take action. This can best be done by avoiding language that unnecessarily generates defensiveness and opposition.
- Write your recommendation so that it can be understood by itself (*e.g.,* the reader will not have to refer to the finding to understand the recommendation).
- Avoid introducing new information in the recommendation that was not presented in the body of the finding. The recommendation should follow logically from what was presented in the finding.
- Avoid extreme language such as "immediately," "without delay," or "as soon as possible." These phrases do not add to the substance of the recommendation. In situations where there is an urgency to correct a problem, include in the recommendation the consequence of delay (*e.g.,* continued loss or waste of money).

The Department of XXXX should XXXX by:

a.

b.

The written Evaluation Report, which contains all findings and recommendations, is issued to legislators and other state and federal officials who have limited time to read reports. Therefore, the Contractor should present findings as concisely as possible, but with enough clarity to be understood by the reader. In addition to being clear and concise, findings should be logical, convincing, and constructive. The findings should be presented in a way that will convince the reader of their significance and motivate the Agency to take action. This is accomplished by clearly presenting the five elements of a finding—condition, criteria, effect, cause, and recommendation.

Although not applicable to this engagement, additional guidance for developing findings can be found in *Government Auditing Standards* issued by the U.S. Comptroller General, which is available online at http://www.gao.gov/.

30. EXHIBIT H - REPORTING REQUIREMENTS AND FORMAT FOR SEPARATELY ISSUED REPORTS

The final Evaluation Report contains findings, conclusions, and recommendations resulting from the Work. It also provides recommendations for changes or modifications to improve the efficiency and effectiveness of the Agency.

Contractor shall prepare the final Evaluation Report in the format delineated below.

REQUIRED REPORTING FORMAT

1. Addressee of Report

   The Evaluation Report should be addressed to "Members of the Legislative Audit Committee."

2. Report Format

   The Evaluation Report will include all of the following sections bound together as a single report and shall be prepared using the OSA format to the extent possible. Acceptable binding formats are limited to spiral, comb, or glued bindings; 3-ring bindings are not acceptable. Contractor may consult the OSA's website for examples of recently issued reports.

   Major sections of the Evaluation Report and their required order within the report are:

   Report Cover
   LAC, Staff, and Distribution Page
   Report Transmittal Letter
   Table of Contents
   Report Highlights
   Overview or Background Chapter
   Findings Chapter(s), Including the Agency's Responses

   a. Report Cover

      The report cover should contain the title and date of the Evaluation Report, including the name of the Contractor conducting the evaluation.

   b. LAC, Staff, and Distribution Page

      The reverse side of the report cover should contain a listing of the current members of the Legislative Audit Committee, OSA staff, and Contractor staff conducting the evaluation. This page also contains information on how to obtain both electronic and bound versions of the report. The distribution information should include the Evaluation Report number. A template will be provided by the OSA.

   c. Report Transmittal Letter

      A letter to the Legislative Audit Committee signifying transmission of the Evaluation Report and signed by the Contractor.

   d. Table of Contents

This page is an index to the report denoting the major report sections and corresponding page numbers.

e. Report Highlights

The highlight sheet is a one-page summary of the report's key conclusions, facts and findings, and recommendations. A template will be provided by the OSA.

g. Overview or Background Chapter

A section of the Evaluation Report, typically presented as a separate chapter, intended to familiarize the reader with the Agency, including its statutory authority and purpose, key functions, organization, descriptive financial and non-financial statistics, etc. This section also includes a general description of the evaluation's purpose, scope, and methodology. This section does not contain the specific background information necessary to establish the evaluation's findings, conclusions, and recommendations.

h. Findings & Recommendations Chapter(s), Including the Agency's Responses

The Evaluation Report must contain this section, typically presented as a separate chapter or chapters, reporting the Contractor's conclusions, findings, and recommendations relative to the evaluation's scope and objectives. See **Exhibit G** for more guidance on developing and presenting findings.

The findings and recommendations included in the report should contain sufficient background to inform a lay reader of the facts and circumstances surrounding the finding. In addition, the findings should identify and emphasize the business effects resulting from the deficiency or instance of non-compliance. Recommendations, which focus on workable solutions that the Agency can effectively implement, are presented after each finding. The recommendations are consecutively numbered and may contain one or more subparts (*e.g.,* 1, 2, 3a, 3b, 3c, 4a, 4b, etc.).

The Agency's formal written response to any recommendations are included in the body of the Evaluation Report following each recommendation. The OSA will provide Contractor with the standard form for obtaining the Agency's responses. The Contractor is responsible for working with the OSA to review the Agency's responses for accuracy, responsiveness to the recommendations, and adherence to the OSA's established parameters. The Agency's responses must be reviewed and approved by the OSA prior to their inclusion in the Evaluation Report. Any "Partially Agree" or "Disagree" responses must include an Evaluator's Addendum, which is a rebuttal to the Agency's response. The language for all Evaluator's Addenda must be reviewed and approved by the OSA prior to their inclusion in the Evaluation Report.

31. EXHIBIT I - SAFEGUARDING REQUIREMENTS FOR FEDERAL TAX INFORMATION

This Addendum regarding Safeguarding Requirements for Federal Tax Information ("Addendum")[1] is an essential part of the agreement between the State and Contractor as described in the Contract to which this Addendum is attached. Unless the context clearly requires a distinction between the Contract and this Addendum, all references to "Contract" shall include this Addendum.

1. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor's employees with the following requirements:

1.1 All work will be done under the supervision of the Contractor or the Contractor's employees.

1.2 The Contractor and the Contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075 and Colorado Revised Statutes 24-50-1002.

1.3 Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.

1.4 All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

1.5 The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of Contractor's computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any FTI remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

1.6 Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the State or the State's designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the State or the State's designee with a statement containing the date of destruction, description of material destroyed, and the method used.

1.7 All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

[1] The language of this Addendum is derived from IRS Publication 1075, *Tax Information Security Guidelines For Federal, State and Local Agencies,* Exhibit 7 – Safeguarding Contract Language, "Contract Language for Technology Services." This Addendum is not exhaustive of all requirements contained in Publication 1075. By agreeing to this Addendum, Contractor agrees to comply with all applicable requirements in Publication 1075 or described on the website of the IRS Safeguards Program, located at www.irs.gov/privacy-disclosure/safeguards-program.

1.8 No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the State, by and through the contracting agency and the Office of Information Technology, and the IRS.[2]

1.9 The Contractor will maintain a list of employees' authorized access. Such list will be provided to the State and, upon request, to the IRS reviewing office.

1.10 The Contractor will not use live FTI in a test environment or utilize a cloud computing model that receives processes, stores, or transmits FTI without express written authorization from the State.[3]

1.11 The Contractor will maintain the confidentiality of all taxpayer information provided by the State or learned in the course of Contractor's duties under this Contract in accordance with safeguards set forth under Colorado Revised Statutes § 39-21-113(4), as amended.

1.12 The Contractor agrees to comply with the following additional requirements in performance of this Contract:

None

1.13 The State will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

2. CRIMINAL/CIVIL SANCTIONS

a. Each officer or employee of any person[4] to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

b. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor

[2] *see* IRS Publication 1075, Exhibit 6 – Contractor 45-Day Notification Procedures.
[3] *see* IRS Publication 1075, Section 9 and www.irs.gov/privacy-disclosure/additional-requirements-for-publication-1075.
[4] The term "person" is used in this Section 2 as it is used in Title 26 of the United States Code and related regulations. The term "person" means a person or entity, including "an individual, a trust, estate, partnership, association, company or corporation." 26 U.S.C. § 7701(a)(1).

punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

c. Additionally, Contractor shall inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractor by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to State records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

d. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the State's security policy and procedures for safeguarding FTI. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the State's files for review. As part of the certification and at least annually afterwards, Contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see *Exhibit 4, Sanctions for Unauthorized Disclosure*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches.[5] For both the initial certification and the annual certification, the Contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

3. INSPECTION

The IRS and the State, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS's right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

[5] *see* IRS Publication 1075, Section 10 or www.irs.gov/privacy-disclosure/reporting-improper-inspections-or-disclosures.