OFFICE OF THE STATE AUDITOR

COLORADO

A Request for Proposals for an IT Performance Audit of Information Security at the Colorado Community College System

November 14, 2025

Table of Contents

Section I Administrative Information....3

Section II Information That Must Be Included in Proposal....18

Section III Proposal Evaluation Process....22

Section IV Supplemental Information....23

Section I Administrative Information

A. Issuing Office

This request for proposals (RFP) is issued by the Colorado Office of the State Auditor (OSA). The terms OSA, State Auditor, 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 audit of information security at the Colorado Community College System.

Colorado Community College System

The Colorado Community College System (CCCS or the System), located in Denver, Colorado, is the state's largest system of higher education, comprising 13 community colleges. Most of the 13 colleges have multiple physical campus locations, in addition to their main campuses, collectively operating over 35 campus locations statewide across Colorado. CCCS serves approximately 125,000 students annually, offering a wide range of academic, technical, and workforce development programs to support Colorado's economic growth and workforce needs. In addition, the Colorado Community College System provides centralized services to the community colleges, such as accounting, budget, legal, and IT.

The 13 colleges in the community college system are as follows:

College	Main Campus Location
Arapahoe Community College (ACC)	Littleton
Colorado Northwestern Community College (CNCC)	Rangely
Community College of Aurora (CCA)	Aurora
Community College of Denver (CCD)	Denver
Front Range Community College (FRCC)	Westminster
Lamar Community College (LCC)	Lamar
Morgan Community College (MCC)	Fort Morgan
Northeastern Junior College (NJC)	Sterling
Otero College (OC)	La Junta
Pikes Peak State College (PPSC)	Colorado Springs
Pueblo Community College (PCC)	Pueblo
Red Rocks Community College (RRCC)	Lakewood
Trinidad State College (TSC)	Trinidad

Average full time equivalent student enrollment and faculty and staff information for three prior consecutive fiscal years, from Fiscal Years 2022 – 2024, are as follows[1]:

Average FTE Student Enrollment from Fiscal Years 2022-2024

Fiscal Years	Resident	Nonresident	Total
2022−2024	43,874	1,912	45,785

Average FTE Faculty and Staff from Fiscal Years 2022-2024

Fiscal Years	Faculty	Staff	Total
2022−2024	3,391	2,084	5,475

CCCS operates under the governance of the State Board for Community Colleges and Occupational Education (SBCCOE or the Board) and was established by the Community College and Occupational Education Act of 1967, Title 23, Article 60 of the Colorado Revised Statutes. The Board functions as a separate entity and, as such, may hold money, land, or other property for any educational institution under its jurisdiction. The statute assigns responsibility and authority to the Board for three major functions, as follows:

- The Board is the governing board of the State system of community colleges.
- The Board administers the occupational education programs of the State at both secondary and postsecondary levels.
- The Board administers the State's program of appropriations to Local District Colleges (LDCs) and Area Vocational Schools (AVSs).

The Board consists of 10 members appointed by the governor to four-year staggered terms of service. The statute requires that board members be selected so as to represent certain economic, political, and geographical constituencies. In addition, there are two nonvoting members consisting of a student representative and a community faculty member.

CCCS's operations and activities are funded primarily through tuition and fees; federal, state, and local grants; the College Opportunity Fund stipends; a fee-for-service contract with the Colorado Department of Higher Education (CDHE); and Amendment 50 funding (extended

[1] Enrollment information was obtained from the Colorado Commission on Higher Education (CCHE), Final Student Full-Time Equivalent (FTE) Enrollment Report. Staff information was obtained from Format 10 and 40 within the Budget Data Book for Fiscal Years 2024 and 2023 that is prepared by higher education institutions for CCHE.

limited game proceeds). In addition, the SBCCOE receives and distributes state appropriations for LDCs, AVSs, and school districts offering vocational programs. Below is a breakdown of the funding allocated to CCCS for Fiscal Year 2025–26, based on the official Colorado Joint Budget Committee Appropriations Report[2].

CCCS Funding Summary (FY 2025–26)

Funding Source	Amount Allocated
General Fund	$228,456,789
Cash Funds	$312,789,432
Federal Funds	$45,123,876
Total Funding	**$586,370,097**

These figures include base operating support, financial aid programs, and workforce development initiatives administered by CCCS.

CCCS Information Technology and Information Security

The CCCS website[3] and published board policies and System procedures[4] indicate that CCCS relies on a complex information technology (IT) environment to deliver online learning, manage student records, support administrative operations, and safeguard sensitive student and employee data. CCCS uses a centralized governance model for System-wide, enterprise technology with clear roles:

- The Board sets policy direction and delegates authority to the System Chancellor.
- The System Chancellor leads the System Office and delegates IT oversight and execution to the System Vice Chancellor for IT/CIO and the college presidents.
- Each college president is responsible for leading implementation of the System-wide policies and procedures locally, ensuring campus alignment with them.

This structure allows CCCS to set consistent standards while giving each college ownership of local execution.

System-wide IT at CCCS, or System IT, operates in an enterprise role, delivering centralized services, shared platforms and infrastructure, and standards that every community college within the System uses, including the following:

- Enterprise applications and integrations (e.g., ERP-adjacent systems, student success platforms)

[2] https://leg.colorado.gov/sites/default/files/fy25-26apprept.pdf
[3] https://cccs.edu/
[4] https://cccs.edu/about/governance/policies-procedures/

- Identity, access, and directory services across the system
- Network architecture standards and shared security controls
- Data and integration standards to support analytics and reporting
- Project intake and prioritization aligned to strategy, risk, and student impact

College-wide IT departments, or College IT, manage local systems and support at each college, whereby each college is expected to bring forward campus needs to CCCS, partner on IT solution design, and operate local services within the shared System-wide enterprise framework.

Similarly, CCCS maintains a centralized, System-wide information security function within the System Office that sets policy, provides shared controls, and leads incident response coordination for the enterprise/CCCS System.[5,6] CCCS's IT and information security functions are separate of the Governor's Office of Information Technology (OIT), which is the State's centralized IT service provider responsible for managing IT resources and service delivery for consolidated state agencies. State agencies consolidated under OIT's authority, as defined by statute, Section 24-37.5-102, C.R.S., include the departments, divisions, commissions, boards, bureaus, and institutions in the executive branch of the state government, including CDHE, **but exclude state-supported institutions of higher education, such as CCCS**. As such, CCCS and institutions of higher education are not required to comply with the information security policies developed and promulgated by the State CISO.

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." CCCS's information security program is overseen by its Chief Technology Officer/Deputy CIO, in conjunction with other members of the IT leadership team, working in coordination with the CDHE and the State's CISO within the Governor's Office of Information Technology (OIT). Under Colorado law, C.R.S. 24-37.5-404.5, institutions of higher education—including CCCS—in coordination with CDHE, must develop an information security program to provide information security for the communication and information resources that support their operations and assets. In accordance with this statute, each institution's information security program must include:

a. Periodic assessments of the risk and magnitude of the harm that could result from a security incident;

b. A process for providing adequate information security for the communication and information resources of the institution of higher education;

[5] https://cccs.edu/about/governance/policies-procedures/bp-6-10-cyber-security-policy/
[6] https://cccs.edu/about/governance/policies-procedures/sp-6-10o-information-technology-continuity/

c. Information security awareness training to inform the employees, administrators, and users at the institution of higher education about the information security risks and the responsibility of employees, administrators, and users to comply with the institution's information security program and the policies, standards, and procedures designed to reduce the security risks;

d. Periodic testing and evaluation of the effectiveness of information security for the institution of higher education, which shall be performed not less than annually;

e. A process for detecting, reporting, and responding to security incidents consistent with the information security policy of the institution of higher education. The institution of higher education, the Colorado commission on higher education, and the State's chief information security officer shall establish the terms and conditions by which the institution of higher education shall report information security incidents to the chief information security officer.

f. Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the institution of higher education in the event of a security incident.

Additionally, C.R.S. 24-37.5-404.5 (3)(b) requires that, every three years, each institution of higher education submit to CDHE a report concerning the development and implementation of the institution's information security program. Specifically, the CDHE shall divide the institutions of higher education into three groups, and each institution of higher education shall submit the required report as follows:

i. The institutions in the first group shall submit the report by July 1, 2020, and by July 1 every three years thereafter;

ii. The institutions in the second group shall submit the report by July 1, 2021, and by July 1 every three years thereafter; and

iii. The institutions in the third group shall submit the report by July 1, 2022, and by July 1 every three years thereafter.

Statute requires that, upon receipt of the reports, CDHE must review the reports and subsequently submit the reports to the State chief information security officer.

C. Services Required

The OSA is soliciting proposals from qualified organizations to conduct an IT performance audit of information security at the Colorado Community College System (CCCS), in accordance with the objectives, scope and methodology outlined in the next section. Subject to oversight and direction provided by the OSA, the engaged firm (Contractor) will be responsible for planning and conducting the audit to obtain sufficient, appropriate evidence necessary to conclude on the audit's objectives, develop complete written findings, write the audit report[7], and present the audit report to the Legislative Audit Committee (LAC), as well as to other legislative committees or oversight bodies, if requested and approved.

The Contractor will conduct this IT performance audit in accordance with generally accepted government auditing standards, issued by the U.S. Comptroller General [see Government Auditing Standards, 2024 Revision].

Audit Objectives, Scope, and Methodology

The objective of this IT performance audit will be to assess CCCS's information security program for compliance with statutory requirements under C.R.S. 24-37.5-404.5, "Institutions of higher education – information security plans." The audit will evaluate whether CCCS has designed and implemented, and is operating an information security program effectively in order to provide adequate protection for the communication and information resources supporting its operations and assets, in accordance with Colorado statutes and other state regulations; CCCS's adopted policies, standards, procedures, or guidelines; and other industry leading practices or standards, as applicable. This audit will include an evaluation of CCCS' oversight of and coordination with the various community colleges within the State's community college system to determine whether CCCS is operating in compliance with C.R.S. 24-37.5-404.5. Specifically, this will include procedures to test the design, implementation, and operating effectiveness, as applicable, of CCCS' information security controls and determine whether CCCS—in coordination with CDHE, has effectively developed its information security program to include:

a. Periodic assessments of the risk and magnitude of the harm that could result from a security incident;

b. A process for providing adequate information security for the communication and information resources of the System;

c. Information security awareness training to inform the employees, administrators, and users at the System about the information security risks and the responsibility of employees, administrators, and users to comply with the System's information security program and the policies, standards, and procedures designed to reduce the security risks;

d. Periodic testing and evaluation of the effectiveness of information security for the System, which shall be performed not less than annually;

[7] Two reports may be necessary to report the findings, conclusions, and recommendations associated with this audit. 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 audit "report" in this document will include the likely possibility of two reports.

e. A process for detecting, reporting, and responding to security incidents consistent with the System's information security policy. The System, the Colorado Commission on Higher Education, and the State's CISO shall establish the terms and conditions by which the System shall report information security incidents to the State's CISO.

f. Plans and procedures to ensure the continuity of operations for information resources that support the System's operations and assets in the event of a security incident.

The audit will also include procedures to determine the System's compliance with the requirements noted in C.R.S. 24-37.5-404.5 (3)(b). This should include determining which of the three groups listed in statute CCCS falls into for when it is required to submit its report to CDHE concerning the development and implementation of the System's information security program, and testing CCCS' compliance with this requirement.

The scope should also include identifying and obtaining an understanding of key CCCS information systems and applications that are subject to the statutory information security requirements and practices, as noted in C.R.S. 24-37.5-404.5, and testing a sample of one or more of these systems and applications for compliance with the requirements and practices, as applicable.

As part of the audit, the Contractor will gain an understanding of CCCS's information security governance and operations in order to plan and develop a detailed, risk-based project scope and methodology to align with the overall project timelines outlined in this RFP. The Contractor will work with the OSA to review and approve its proposed scope and methodology, prior to engaging in the fieldwork steps necessary to achieve the audit objective. The audit methodology may include inquiries of management and staff, observations of relevant processes and controls, inspections of supporting documentation and evidence, and reperformance of processes and controls, as deemed necessary to achieve the audit objective.

The audit scope will include those System-wide and/or campus IT and information security governance structures, policies, standards, procedures, and practices that are overseen and managed by CCCS. Applicable CCCS IT and information security related practices at each of CCCS' 13 colleges may be included, to the extent that they relate to the objectives of the audit (e.g., if CCCS is responsible for integrating, managing, or enforcing these practices), and if deemed appropriate by the Contractor and OSA based on the Contractor's risk assessment and discussions with OSA during the planning of the audit. However, procedures to evaluate the IT and information security practices at CCCS's 13 colleges should be considered outside of the scope of this audit. Similarly, applicable CCCS IT and information security related vendor management practices may be included, to the extent that they relate to the objectives of the audit (e.g., if CCCS is responsible for integrating, managing, or enforcing these practices), and if deemed appropriate by the Contractor and OSA based on the Contractor's risk assessment and discussions with OSA during the planning of the audit. However, procedures to evaluate the IT and information security practices of CCCS's third party vendors and/or service providers should be considered outside of the scope of this audit.

Subject to oversight and direction provided by the OSA, the Contractor will be responsible for planning and conducting the audit to obtain sufficient, appropriate evidence necessary to conclude on the audit's objectives, develop complete written findings, write the audit report, and present the audit report to the Legislative Audit Committee (LAC), as well as to other legislative committees or oversight bodies, if requested and approved.

Deliverables and Timelines

The OSA expects the Contactor to satisfy the project deliverables and timelines outlined in this RFP to meet a December 2026 Legislative Audit Committee hearing date, at which point the audit 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., Joint Technology Committee or others), upon request and approval of the LAC. **The Contractor must attend the Legislative Audit Committee hearing, and any additional presentations that may be requested and approved, in person to present the final audit report.**

Work for this project is estimated to commence approximately the week of January 23, 2026. 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 billable work can begin on this project until the effective date of the contract.**

Work Location

Depending on the needs of the engagement or the nature of work being performed, some work for this engagement may be able to be completed using email, phone, and other virtual file-sharing and remote meeting technologies. However, some amount of in-person or on-site work at CCCS and its campuses may also be required. The Contractor will work directly with CCCS during the engagement, and the OSA contract monitor, if needed, to determine an appropriate work location necessary to complete the services requested and the various related work tasks to meet the audit objective.

Planning and Fieldwork

The planning and fieldwork phases of this project are expected to take place from approximately the weeks of January 26, 2026 through June 22, 2026 and include the following project deliverables and timelines:

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.	1/26/2026
Hold Entrance Conference with CCCS	Hold an in-person entrance conference with the appropriate CCCS personnel to discuss the audit, timeline, and logistics. The OSA contract monitor and State Auditor participate in this meeting. The Contractor is responsible for scheduling this meeting with the assistance of the OSA contract monitor.	2/2/2026
Gain Understanding and Develop, Risk-Based Project Scope and Methodology	Gain an understanding of CCCS operations, requirements, and criteria, and develop a detailed, risk-based project scope and methodology to align with the overall project timelines outlined in this RFP. Provide the scope and methodology to the OSA contract monitor for review and approval, prior to beginning fieldwork.	2/23/2026
Begin Fieldwork **Note:** Fieldwork can begin as soon as possible and when ready after the project scope and methodology are approved by the OSA.	Obtain and review documentation, interview CCCS personnel and others as appropriate, and analyze data. Have ongoing communication with CCCS throughout fieldwork to ensure a clear understanding of operations, requirements, and criteria; request documentation and perform test procedures; clear results and any identified exceptions; and update on status and logistics.	3/2/2026
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 CCCS. 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 3/9/2026 and ongoing regularly (e.g., bi-weekly, etc.) through the completion of the contract 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 CCCS before any associated findings are developed.	6/22/2026

Findings and 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 CCCS. 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. The final 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. The OSA's standard contract containing both exhibits 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 reports 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 June 22 through December 7, 2026 and includes the following project deliverables and timelines:

Tasks	**Details**	**Completed Approximately by the Week of:**
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 and/or work performed may occur as the draft written findings are discussed, reviewed, revised.**	6/29/2026
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.**	7/20/2026
Coordinate with the OSA Contract Monitor to Submit Written Findings to CCCS	Once the written findings are approved by the State Auditor, coordinate with the OSA contract monitor to submit the written findings to CCCS for review prior to the findings clearing meeting. The written findings should be provided to CCCS 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.	8/3/2026
Hold Findings Clearing Meeting with CCCS	Hold an in-person findings clearing meeting with CCCS to discuss CCCS'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 Contractor should attend these meetings in person.	8/10/2026
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 audit, there will likely be two audit 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.	8/17/2026

Tasks	**Details**	**Completed Approximately by the Week of:**
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.	8/31/2026
Submit Draft Report to CCCS	Once the draft report is approved by the State Auditor, coordinate with the OSA contract monitor to submit the draft report to CCCS for review prior to the exit conference and to begin preparing its written responses to any recommendations. The draft report should be provided to CCCS at least 1 week prior to the exit conference.	9/21/2026
Hold Exit Conference with CCCS	Hold an in-person exit conference with CCCS to obtain and discuss feedback on the draft report and CCCS'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 CCCS. All report changes must be reviewed and approved by the OSA before submitting the revised draft to CCCS.	10/5/2026
Obtain Written Responses from CCCS	Coordinate with the OSA contract monitor to obtain and review CCCS's written responses to recommendations and, once obtained, work with the OSA to revise the report narrative, suggest revisions to CCCS's responses, and prepare Auditor's Addenda, as appropriate (i.e., for any disagreement or partial agreement from CCCS to the reported recommendations).	10/12/2026
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 11/2/2026. OSA to provide approval to print no later than approximately 11/9/2026.
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: • An electronic copy of the final report file in unprotected PDF format. • Up to 50 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	11/16/2026 **Note:** This task should be completed **no later than** the date noted, instead of approximately by

Tasks	Details	Completed Approximately by the Week of:
	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 CCCS in advance of the hearing.	the week of the date noted.
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 up to two dry runs of the Contractor's presentation with the OSA contract monitor to practice the presentation and incorporate suggested revisions. The dry run(s) 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.	11/16/2026
Present Report to the Legislative Audit Committee	Provide in-person oral testimony to the Legislative Audit Committee summarizing the report's findings, conclusions, and recommendations and responding to questions from Committee members. The Contractor may also be required to present in-person oral testimony to other oversight bodies or legislative committees (e.g., Joint Technology Committee, CCCS's Board, etc.), if requested and approved. Audit report hearings typically last 1 to 2 hours, but could be longer or shorter depending on the report's contents.	Approximately 12/7/2026

D. Schedule

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

1. RFP available to prospective bidders	Friday, November 14, 2025
2. Prospective bidders' inquiry deadline (5:00 p.m.MT)	**Friday, November 21, 2025**
3. OSA response to inquiries deadline	Friday, December 5, 2025
4. Proposal submission deadline (5:00 p.m. MT)	**Friday, December 12, 2025**
5. Approximate bid selection date	Friday, January 9, 2026
6. Approximate contract date	Friday, January 23, 2026

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@coleg.gov. **No inquiries will be accepted after 5:00 p.m. MT on 11/21/2025.**

F. Submission of Proposals

Proposals must be submitted via email to Matt Devlin, Contract Monitor, at matt.devlin@coleg.gov. **No proposals will be accepted after 5:00 p.m. MT on 12/12/2025.**

All proposals become the property of the OSA upon receipt and will not be returned to the bidder. The OSA 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 OSA 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 OSA 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 the OSA determines that it is in the best interest of the State to do so. The lowest cost proposal will not necessarily be selected. The OSA also reserves the right to engage in further negotiation of the project scope of work, price, and contract terms after selection of the Contractor if the OSA determines that it is in the best interest of the State to do so.

H. Addendum or Supplement to Request for Proposals

The OSA 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 known prospective bidder.

I. Award Without Discussion

The OSA 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 OSA 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. OSA Contract Monitor

The OSA will assign a contract monitor to serve as the Contractor's primary point of contact and liaison throughout the project. The contract monitor will attend all key Department/agency meetings during the engagement (e.g., entrance/exit conferences, findings clearing meetings, briefing meetings with management or boards/commissions, Legislative Audit Committee hearing); assist the Contractor in understanding the OSA's requirements, processes, and expectations; and facilitate the OSA's review of project deliverables, including providing guidance and feedback for revisions.

M. Award of Bid

The contract will be awarded to the bidder whose proposal the OSA determines to be the most advantageous to the State of Colorado.

N. Submission of Invoices

The Contractor must submit monthly invoices for audit work completed. The OSA will withhold payment for 10 percent of the total contract amount pending satisfactory completion of the contract scope of work, which typically occurs after the Legislative Audit Committee hearing when the final report is publicly released.

Section II Required Information

A. Proposal Sections

Proposals must include the following information. Failure to provide all required information may result in disqualification of the proposal.

1. Title Page

Identify the RFP being responded to and the responding organization's name, local address, telephone number, contact person, and date.

2. Table of Contents

List the material included in the proposal by section and page number.

3. Transmittal Letter

Include a transmittal letter to no more than two pages. The transmittal letter must include the names of the individual(s) authorized to make representations for the organization and their title(s), mailing address(es), email address(es), and telephone number(s).

4. Profile of the Organization

This section of the proposal must:

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

b. 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.

c. 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.

d. Describe any and all work that (i) is currently being performed for CCCS, any of its community colleges, or the State of Colorado, (ii) was performed for CCCS, any of its community colleges, or the State of Colorado within the past 2 years (i.e., October 2023 – October 2025), and (iii) is planned for CCCS, any of its community colleges, or the State of Colorado (i.e., proposals submitted for work that has not yet been awarded or contracted).

e. Affirm that the organization is independent for this audit engagement.

Prior, current, or planned work disclosed pursuant to Item #4(d) may create a threat to independence. In affirming the organization's independence for this audit engagement, the proposal must include explanation/analysis, in accordance with the independence framework prescribed in Government Auditing Standards, why this prior, current, or planned work would not impair the organization's independence—or create the appearance thereof—in performing this audit.

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

g. 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.

h. Provide a copy of the results of the organization's most recent external peer review, as the organization will conduct this audit in accordance with generally accepted government auditing standards.

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

5. Qualifications of Assigned Personnel

Describe the proposed audit 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 audit, including any specialists or subcontractors to be used. The proposal must include a resume of all principal staff highlighting their professional qualifications and similar audit 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.

6. Organization's Approach to the Audit

Include a description of the proposed work plan for the audit engagement, including proposed audit procedures, steps, methodologies, approaches, tools, and resources to (a) conduct the audit, (b) ensure fully developed findings, and (c) conclude on the audit objectives based on sufficient, appropriate evidence.

The proposal must indicate that the organization will conduct the project in accordance with generally accepted government auditing standards, as well as any other applicable professional standards to which the organization will adhere.

7. **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 (see Section IV–Supplemental Information).

   Bidders should not wait until after the OSA has made a contract award to consult with their legal team/advisor about the contract terms and conditions. Bidders must identify and describe any issues with the terms and conditions in the OSA's standard contract and its related exhibits as part of their proposal, including proposing alternative language if appropriate. The OSA will consider this information when evaluating proposals and making the contract award.

8. **Compensation and Staff Hours**

   This section of the proposal must:

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

   b. Break out total hours estimated to (i) complete each issue/objective, (ii) write findings, and (iii) write and finalize the audit report.

   c. State the total inclusive maximum fee for which the work requested will be done.

   d. Affirm that all prices, terms, and conditions will be held firm for at least 90 days after the bid opening.

9. **Delivery Schedule**

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

10. **Additional Data**

    Include additional information that is considered essential to the proposal but has not otherwise been provided in response to a specific item in this section.

B. Separate Redacted Proposal for Proposals Containing Proprietary Information

All proposals submitted to the OSA in response to this RFP are subject to the Colorado Open Records Act (CORA). In accordance with CORA, bidders may request that the OSA withhold proprietary information (e.g., trade secrets) in their proposals from public disclosure pursuant to a CORA request.

Bidders requesting that the OSA withhold proprietary information in their proposal from public disclosure pursuant to a CORA request must prepare and submit a separate redacted copy of their proposal to the OSA. In no event may an entire proposal be classified as proprietary information.

The OSA will review any designations of proprietary information for reasonableness and appropriateness as part of its review of proposals. If the OSA does not agree with the bidder's designation of proprietary information, the bidder will be notified and asked to provide additional explanation and clarification and, if necessary, refine what is designated as proprietary information and submit a revised redacted proposal.

Section III Proposal Evaluation Process

A. General

An OSA evaluation team will judge the merits of proposals received in accordance with the evaluation criteria defined below.

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.

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

B. Mandatory Criteria

1. The organization is independent for the audit engagement.

C. General Criteria

1. Adequacy and completeness of the proposal with respect to the information required by Section II of the RFP.

2. Qualifications and experience of personnel, including any subcontractors, specialists, or consultants, assigned to the audit team.

3. Comprehensiveness and appropriateness of the proposed work plan.

4. Proposed hours and cost.

5. Acceptance of the OSA's standard contract and its related exhibits without significant revision.

Section IV Supplemental Information

Attached to this RFP are the following documents:

1. Standard OSA contract and related exhibits. See Section II(G) of the RFP for discussion. The State is developing the standard OSA contract document in an accessible format and in compliance with the state's accessibility rules. The State will provide an accessible version of the standard OSA contract document to the Contractor after the State has completed development of the standard OSA contract document in an accessible format. The accessible OSA contract document will not change or amend any substantive terms of the standard OSA contract that is attached to this RFP.

Note: To view the contract template, please be sure to download the RFP, save the pdf, and then open the saved file in Acrobat. You should be able to see the contract template and the exhibits as attachments. If you can't see the attachments, click the paperclip icon. (You will not see linked attachments in a pdf preview.)

The following web links provide additional information that relate to information noted in this RFP or that may be useful to potential bidders as they prepare their proposals:

- Colorado Office of the State Auditor Website:

  http://www.colorado.gov/auditor

- Colorado Community College System Website:

  https://cccs.edu/

- Colorado Community College System, Board Policies & System Procedures (including Series 6: Information Technology) Website:

  https://cccs.edu/about/governance/policies-procedures/

- OSA Cybersecurity Resiliency at the Judicial Department — Public Report

  https://leg.colorado.gov/audits/cybersecurity-resiliency-judicial-department-%E2%80%94-public-report

- OSA Evaluation of Cybersecurity Maturity Model Certification (CMMC) Readiness at the Colorado State University System — Public Report

  https://leg.colorado.gov/audits/evaluation-cybersecurity-maturity-model-certification-cmmc-readiness-colorado-state

- OSA IT Performance Audit of Cybersecurity Resiliency at the Governor's Office of Information Technology — Public Report:

  https://leg.colorado.gov/audits/audit-cybersecurity-resiliency-governors-office-information-technology-—-public-report

- OSA IT Performance Evaluation Report Example: Evaluation of IT Service Management at the Governor’s Office of Information Technology, February 2022.

  https://leg.colorado.gov/audits/information-technology-service-management