FY 2026-27 IT Capital Budget Requests
Combined Staff Analyses

Fiscal Year 2026-27 IT Capital Budget Request

Arapahoe Community College
System Replacement

Project Summary

Arapahoe Community College (ACC) is requesting state funds to acquire and install replacement classroom technology.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$1,174,447	$1,195,666	$1,056,698	$3,426,811
CF	$0	$137,000	$137,000	$137,000	$411,000
Total	**$0**	**$1,311,447**	**$1,332,666**	**$1,193,668**	**$3,837,811**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Department of Higher Education	1 of 10 (tied)	Recommended for funding.

Project Status

This is a new never-before-requested project for state funds to fund phase one of a new, three-phase project.

Project Information

Project Objective

The project will replace existing classroom and conference room technology with new components, including projectors, screens, and peripherals as needed. Current technology is past its useful lifespan and lacks standardization. According to ACC, the replacement of classroom and conference room technology will enhance delivery of remote instruction, benefitting students and faculty.

Project Description

This request is for phase one. ACC will make requests for a total of three years to replace all classroom technology, with each year of funding replacing technology in a portion of campus buildings. Phase one replaces technology in 21 rooms, phase two replaces 22 rooms, and phase three replaces 23 rooms. A total of 66 rooms at the Littleton and Castle Rock campuses will receive new technology. The average cost per room is about $60,000, which includes equipment and installation costs.

ACC will use vendors to procure the items and modify rooms for installation as needed. Deployment of new technology will occur in coordination with IT and Facilities Departments to ensure functionality when technology is brought online. If funding is not provided in future years, then ACC will add new technology within existing resources as existing technology fails.

Project Planning

ACC's IT department generated cost estimates by using vendor quotations. Contractors will be used to install equipment and make necessary changes to rooms for installation. No additional ACC FTE are required for this project. The expected lifespan of the new technology will be about 10 years, with ACC responsible for maintenance. As new technology is installed, ACC will decommission and surplus existing technology. The potential maintenance and operating costs will be absorbed within the existing ACC IT Department budget.

Overall, JTC staff believes the project planning for this project is scaled from ACC's usual procurement process. Additionally, ACC will offer annual trainings for faculty and staff on the new technology and is prepared to conduct additional trainings as necessary.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$297,200	$285,400	$265,600	$848,200
Equipment	$0	$951,797	$983,806	$871,255	$2,806,858
Contingency	$0	$62,450	$63,560	$56,843	$182,853
Total	**$0**	**$1,311,447**	**$1,332,766**	**$1,193,698**	**$3,837,911**

Cost Benefit Analysis

ACC was unable to quantify cost savings as required by Section 24-37-304 (1)(c.5)(V), C.R.S., but reports that the primary benefit of the project is avoiding the inefficiencies of its current technology. New technology will result in fewer downtime incidents, be energy efficient, and covered by warranties that have not expired. The new technology will improve student experience, leading to higher retention of students and other improved educational outcomes.

Cash Funds

The source of ACC cash funds for the project is ACC general funds.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Design—Phase 1	July 2026	July 2026
Construction—Phase 1	August 2026	June 2027
Design—Phase 2	July 2027	July 2027
Construction—Phase two	August 2027	June 2028
Design—Phase three	July 2028	July 2028
Construction—Phase three	August 2028	June 2029

Staff Questions and Comments

Project Questions

Q: Are there any master agreements that ACC can use for this project?

A: There are state vendor/price agreements that can be used.

Technical Questions

Q: Has the College received competitive quotes on the replacement technology for these classrooms? Please describe information on the vendor selection and any other market research.

A: Yes. We have worked with multiple vendors and suppliers of the products we will be using to review pricing and support for the materials we would be purchasing. This helped us obtain information for our application.

Q: Has the College looked into other vendors than Cisco for its new switches, such as Juniper, for possible cost savings?

A: Cisco is a CCCS system-wide standard.

Q: Will all classrooms that require upgrading equipment, have the exact replacement equipment and technology moving forward? Will all 6 security features listed in the Additional Information Section (Enhanced Security Features, Network Segmentation, Access Control, Regular Updates and Patches, Improved Monitoring and Logging and Compliance with Security Standards) be fully implemented in each classroom?

A: Yes, classrooms will have the same equipment. Yes, all six security features will be fully implemented in each classroom.

Q: Will the cost of the ISP provider to the campus be compared to other vendors for possible cost savings?

A: The CCCS System Office provides network service to all ACC campuses through the CCCS Wide Area Network (WAN).

Q: Will the system provide proactive alerts on system events?

A: To some extent, there will be alerts. There will also be remote troubleshooting capabilities.

Q: Will the system support user authentication, password policy management, two-factor authorization, single sign-on and role-based access?

A: The management of the system has security features. Since it is AV, the user will not interact with features that require authentication, MFA, or SSO.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: This AV system will interface with computing equipment (instructor and/or student) and allow the seamless presentation of content and collaboration between stakeholders in the room and remotely.

Fiscal Year 2026-27 IT Capital Budget Request

Colorado Mesa University
Student Information System Modernization

Project Summary

Colorado Mesa University (CMU) is requesting a combination of state funds and cash fund spending authority to replace the Student Information System (SIS).

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$8,316,655	$0	$0	$8,316,655
CF	$0	$535,559	$0	$0	$535,559
Total	**$0**	**$8,852,214**	**$0**	**$0**	**$8,852,214**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 10	Not recommended for funding.
Colorado Commission on Higher Education	5 of 10	Recommended for funding.

Project Status

This is new, never-before-requested project. In FY 2023-24, CMU was awarded $3.6 million in state and cash funding spending authority to implement a cloud software-as-a-service (SaaS) human resources and finance resource planning systems and develop a data management and data integration strategy.

Project Information

Project Objective

CMU will complete a system replacement of the current SIS. This system is responsible for storing academic records, student scheduling and registration, student accounts and billing, financial aid, academic advising, degree planning, and other administrative tasks. Upgrading the system will provide a more user friendly experience, increased student engagement, and operational efficiency and effectiveness.

Project Description

This project will occur in a single phase and will accomplish the following:

- implement a SaaS that will provide a core solution that manages all student-related business capabilities;
- digitally transform the user experience and streamline administrative processes;
- eliminate third party software and databases licenses;
- reduce staff time allocating toward maintaining and supporting the current system; and
- leverage the previous efforts made by CMU to invest in a data management platform to build a student system that will work together seamlessly.

CMU states it will assist students through not only a more streamlined and cohesive project, but also hopefully save the students money. A modernized platform will provide a more transparent outline of degree requirements, tracking courses, and help assist with building degree plans to avoid unnecessary courses. Additionally, faculty is expected to have increased student engagement and improve student learning outcomes. Benefits for staff include streamlined administrative processes and more innovation with evolving IT through technology like artificial intelligence. Finally, the university will benefit by vendors providing ongoing maintenance as well as cost savings by eliminating expensive, outdated third party software and database licenses.

When asked by staff if the project could be split into several phases, CMU stated that splitting the project up will lead to inefficiencies and increased costs, and the current timeline of the project lines up with the academic calendar.

Project Planning

CMU states that a Request for Proposal (RFP) will be initiated to deliver designated requirements. Prior to the RFP, the project will start with a consultant, working to:

- identify system capabilities and requirements pre-implementation;
- develop the project management approach; and,
- establish the university's goals.

Through the money appropriated in FY 2023-24, CMU was able to develop a more comprehensive digital transformation plan, which will leverage the recent upgrades and expand to student services. Additionally, CMU collaborated with a number of other Colorado universities in monthly calls to exchange information and insight on project benefits, costs, and lessons learned on ERP and SIS modernization projects.

The new system has a life expectancy of 10 to 15 years. The only cost to decommission the system will be phasing out of current software agreements which will have no impact on the project cost. CMU anticipates between five and eight years of historical data will be migrated and the rest will be archived in CMU's data management platform/warehouse. During implementation, CMU will maintain its legacy system and two years of the SaaS subscription cost is included in the request in order to support both systems. This cost will then be assumed by the institution as an operating request.

The vendor will be required to provide 24/7 technical support as well as training and assistance for users. This will include online training materials, training sessions during system implementation, and user-training and support embedded throughout the system.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$6,415,935	$0	$0	$6,415,935
Software	$0	$1,343,266	$0	$0	$1,343,266
Contingency	$0	$387,960	$0	$0	$387,960
ADLE	$0	$705,053	$0	$0	$705,053
Total	**$0**	**$8,852,214**	**$0**	**$0**	**$8,852,214**

Staff inquired about the cost of the project potentially being decreased. CMU stated that the university has worked diligently on identifying all potential costs and was not able to find any reductions. The university is continuing to explore ways to reduce the time allocated to the

pre-design, planning, and procurement phases, but notes they are reluctant to make any changes.

Cost Benefit Analysis

CMU projects that the new SIS system will bring annual savings of $4,730. These savings are attributed to eliminating the current infrastructure and database expenses, support and subscription agreements, and the amount of time spent by staff on technical support for electronic forms.

Cash Funds

The source of these cash funds is university reserves.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	April 2026	June 2026
Readiness Planning	June 2026	October 2026
Procurement	July 2026	October 2026
Design	September 2026	October 2026
Implementation	October 2026	December 2028

Staff Questions and Comments

Technical Questions

Q: In the F. Assumptions for Calculations section, did the 3 vendors who provided estimates for implementing SIS Software-as-a-Service (SaaS) that included implementation services respond to an RFI/RFP/RFQ how were these estimates obtained?

A: CMU obtained the estimates through its RFP process for HR and Finance Software and System Integration Services. Some ERP vendors included SIS options in their proposals. The University asked the vendors for additional information to finalize its cost and product benefit comparison.

Q: Are all 40+ software applications that exchange data with the legacy Banner system going to be implemented into the new SIS SaaS system?

A: CMU aims to replace as many of the 40+ applications as possible with the base SIS SaaS suite. However, some applications essential to managing specific business areas will continue to be used after the SIS SaaS implementation. For instance, Residence Life will keep using its residence hall management software, and Student Life will maintain its student conduct software. Both applications receive student course schedule data from the University's SIS to support student engagement.

CMU plans to eliminate more than a dozen applications, which include the legacy Banner SIS applications. Eliminating applications has been factored into the savings estimate. Additionally, the University expects to identify further efficiencies and opportunities to consolidate applications through the project's Organization Change Management process.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: A requirement for the University selecting its SIS SaaS product is that it meets all integration requirements. CMU will handle integrations through direct Application Integration Interfaces (APIs) and/or the University's data management platform. CMU is 100% confident that this can be accomplished based on what the University has learned through its current ERP Modernization Project.

Q: Will the system provide proactive alerts on system events?

A: Yes. CMU will require the SIS SaaS vendor to provide proactive alerts and notifications for key system events to ensure timely awareness and response to potential issues or performance impacts. The requirements for monitoring system events and sending alerts will be addressed during the RFP process and will be in the contractual agreement with the vendor.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: CMU will require that the selected SIS SaaS product supports strong authentication methods, including multifactor authentication. The University utilizes Secure Assertion Markup Language (SAML) for single sign-on functionality to both on-premises and cloud-based applications, and Microsoft Authenticator for multifactor authentication across academic and business applications. CMU will require the vendor's product to integrate with the University's identity management system to manage role-based access to the SIS. CMU has found that modern enterprise applications meet these requirements without difficulty.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: CMU will utilize the extensibility platform of the selected SIS SaaS product to create low-code / no-code custom applications and enhance the user interface with new functionality. This will leverage the core product's data, security, and workflow logic. The extensibility platform will enable the university to tailor the SIS to meet its specific business processes and data requirements while maintaining the reliability, agility, accessibility, and security of the SaaS product. Additionally, this approach will allow CMU to benefit from faster feature releases, timely security updates, and the innovation capabilities of modern SIS SaaS products, which are often lost in highly code-customized applications.

Q: Before awarding the vendor a contract, will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes. The process of assessing vendor health and financial position begins with RFP responses. CMU's standard IT services RFP template includes a set of questions to evaluate the vendor's performance record and financial stability. These questions aim to determine if the vendor is for sale or involved in any transactions related to expansion or acquisition by another business entity. Additionally, it addresses any past or impending litigation or claims filed against the vendor that could negatively affect its performance under an agreement with the University. Finally, the questions inquire whether the vendor is currently in default of any loan or financing agreement with banks, financial institutions, or other entities.

Q: Will you be asking the selected vendor to provide a minimum of two high quality references of their work with higher education institutions?

A; Yes. CMU's standard RFP template for IT services requires vendors to provide history and references from at least three (3) clients, highlighting any higher education customers that currently use the proposed solution or services. The University is committed to evaluating the quality of the product and the performance of the implementation, and it will verify references before award. Additionally, CMU may reach out to institutions not included in the reference list to gain a broader perspective. This outreach would include contacting other Colorado institutions that work with the vendor.

Fiscal Year 2026-27 IT Capital Budget Request

Colorado Northwestern Community College
Security Camera Upgrades

Project Summary

Colorado Northwestern Community College (CNCC) is requesting state funds for a security cameras upgrade that includes cabling, network equipment, and software licensing for both CNCC campus locations.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$986,192	$0	$0	$986,192
CF	$0	$0	$0	$0	$0
Total	**$0**	**$986,192**	**$0**	**$0**	**$986,192**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Colorado Commission on Higher Education	6 of 10	Recommended for funding.

Project Status

CNCC is requesting state funds for a single-phase project.

Separate from this request, the college was appropriated $571,163 in FY 2025-26 for its Campus Redundancy Upgrade project and was part of the Rural College Consortium with five other colleges, which received an $8.6 million appropriation in FY 2022-23 for IT Infrastructure. Finally, CNCC was appropriated $1.7 million in state funds and cash fund spending authority in FY 2021-22 for a Network and Security Upgrade, which allowed the college to purchase Meraki cameras on the Rangely campus.

Project Information

Project Objective

The project aims to increase security at the Craig and Rangely campuses through the purchase and installation of new cameras and equipment. The college states that existing surveillance infrastructure is 15 to 25 years old, reaching end of life, and placing inefficient time demands on IT and security personnel. The existing system operates on three separate management systems across the two campuses and the upgrade will align all security cameras to a single system. Additional challenges include degraded image quality, outdated software, and a growing number of camera failures. When asked by staff about the extent of unreliability of the current system, CNCC reported that cameras are starting to fail due to age and that they have blind spots at certain entrances. CNCC further states that the Craig campus utilizes low-definition coax cameras originally installed in 2010.

CNCC reports that the request is responsive to a federal law concerning campus security requirements to have sufficient video coverage, quality, and storage capacity. According to the college, the existing system provides inadequate and unreliable access to local law enforcement. The project will address these issues and provide a more modern and reliable security system.

Project Description

CNCC states that the project supports the IT department's strategic plan. Coaxial cable will be replaced with CAT6 structured cables to support new switches, sensors, and cameras across all buildings and parking lots on the Craig Campus. New cameras will be installed in two buildings that are currently unsupported on the Rangely campus.

While existing cameras as part of the request are roughly 15 years old, CNCC indicates that the lifespan of the new equipment is generally five to ten years. According to CNCC, the project will follow a milestone-based schedule with weekly progress meetings, punch list tracking, and variance monitoring to maintain control over scope, timeline, and budget.

Project Planning

CNCC arrived at project costs through vendor quotes and historical estimating data from past controlled maintenance projects with similar scopes. CNCC also states that it will implement a competitive procurement process with prequalification and technical scoring, ensuring vendor competency and pricing transparency

Training for the system will be minimal because the college is currently using an existing Cisco Meraki dashboard, which will apply to the new system. CNCC manages training in-house. CNCC states that the college has been using similar equipment in other locations since 2022, which the college installed as the result of the prior capital appropriation mentioned above.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$166,902	$0	$0	$166,902
Software	$0	$551,309	$0	$0	$551,309
Equipment	$0	$168,137	$0	$0	$168,137
Contingency	$0	$88,635	$0	$0	$88,635
ADLE	$0	$11,209	$0	$0	$11,209
Total	**$0**	**$986,192**	**$0**	**$0**	**$986,192**

Cost Benefit Analysis

CNCC did not provide a cost-benefit analysis in the request, but notes that licensing associated with the project will increase IT operating budget by 15 percent. CNCC states that at the same time, it will lower operational costs by standardizing and centralizing four operating systems into one system.

In response to a follow-up inquiry from staff, CNCC described that the project will add extra safety measures while also reducing manual patrol time, response time to alerts, and incident investigation time. The college states that financial savings will also accrue from reduced property loss and damage, reduction in vandalism and decreased property theft. CNCC further states that by having their internal IT team install, configure, and network the cameras, cost

savings between $50,000 and $100,000 may be realized as compared to having work completed via a contractor, which the college estimates costing roughly $5,000 per day.

Cash Funds

The project does not include a cash fund component. Of note, the Colorado Commission on Higher Education (CCHE) uses scoring criteria for ranking higher education institution projects. The ranking includes an "Other Fund Sources" component, which incentivizes institutions in contributing cash funds in their requests. However, CCHE exempts certain institutions including CNCC from this metric. CNCC does state that in lieu of cash, the college is using IT staff for setup and installation to save costs, as described above.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Design	July 2026	December 2026
Construction	February 2027	September 2027
Equipment	September 2027	November 2027
Occupancy	December 2027	December 2027

Staff Questions and Comments

Staff Comments

In addition to be appropriated funding in FY 2025-26 and separate from this request, the college provided a 5-year plan that includes other projected IT capital requests. Over the following two fiscal years, CNCC plans requests of $584,769 for a server room upgrade and $360,000 for classroom IT systems, respectively.

Project Questions

Q: The request states that 3-year roll-forward spending authority is not required. However, the timeline suggests the project completion as December 2027. Is the college confident that all funds will be encumbered by the completion of FY 2026-27?

A: Yes, the bulk of the funding will be used for the cameras and licensing, and these can be ordered immediately after funding. Contractor work will be limited to replacing old coax cabling and running new cabling for external cameras.

Technical Questions

Q: Will there be or is there a current policy in place for video data storage? For example:

- Minimum Retention;
- Security; Date stored in a secure controlled location limited to authorized personnel;
- Data Access; Access to footage is restricted;
- Purpose and Privacy; Surveillance is primarily for crime deterrence and investigation; and
- Extended Storage; Under certain conditions data footage can be kept longer than your standard policy set?

A: Responses for each component of data storage are as follows:

- Minimum Retention; Yes, to meet Title IX requirements, CNCC retains 90 Days of video recordings;
- Security; Meraki camera recordings are stored locally on the camera and can only be accessed through the Cisco Meraki Dashboard;
- Data Access; Yes, access is restricted to specific users assigned in the Cisco Meraki Dashboard;
- Purpose and Privacy; Yes, due to limited security personnel, cameras are used for deterrence and investigating any potential incident brought to our attention; and
- Extended Storage; Longer storage involves saving incident recordings off the Meraki camera and storing it on a campus server. The cameras are also set to only retain recordings with motion and can regularly hold over 90 days of motion incidents. Another possibility is to purchase cloud storage for over 90 days and assign it to the cameras that need it.

Q: Will the system enable logging and resolution reporting on all issues (cybersecurity)?

A: The Cisco Meraki Dashboard logs user and equipment activity/events. This includes any changes made to cameras. Resolution reporting is limited to system alerts/errors. The Cisco Meraki Dashboard does not include a reporting space for recorded events and must be done outside of the dashboard.

Q: Will the new video system provide proactive alerts on system events?

A: System events are logged and can be set to notify based on the type of event. Camera Alerts can also be customized on a per camera basis.

Q: Will the new video System support user authentication, password policy management, two-factor authorization, single sign-on and role-based access?

A: The Cisco Meraki Dashboard supports user authentication, SSO, password management, and two-factor authentication. Role based access is limited to full camera access and view only access. Any further camera access restrictions are managed by creating separate networks in the dashboard.

Q: Will the vendor provide technical support e.g. 24/7 tech support?

A: Yes, Cisco Meraki includes 24/7 tech support.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Community College of Aurora

Modernizing Campus Technology and Life Safety

Project Summary

The Community College of Aurora (CCA) is requesting a combination of state and cash funding spending authority to enhance disaster recovery, modernize learning environments, and improve campus safety.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$949,050	$1,899,050	$949,050	$3,797,150
CF	$0	$49,950	$99,950	$49.950	$199,850
Total	**$0**	**$999,000**	**$1,999,000**	**$999,000**	**$3,997,000**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Colorado Commission on Higher Education	10 of 10	Recommended for funding.

Project Status

This is phase one of three for a new, never-before-requested project.

CCA was appropriated $855,000 from a combination of cash and state funding in FY 2023-24 for the Improving Server Room project and $529,000 in FY 2022-23 for the Improving Student Access to Technology project.

Project Information

Project Objective

This request is broken down into three phases that address different IT systems combined into one request. The completion of the project would result in strengthening disaster recovery, replace obsolete technology, and enhance life safety systems.

Project Description

Phase one of the project, considered here, will focus on addressing vulnerabilities and creating a modern disaster recovery plan. CCA cited vulnerabilities such as an aging laptop fleet that consists of end-of-life devices that are no longer supported by manufacturers and inadequate disaster recovery abilities. In the event of a cyberattack or other disaster, CCA could face very extensive downtime.

This phase of the project will complete the following actions:

- engage with a consultant to develop and implement a disaster recovery plan;
- upgrade systems and network components; and,
- establish ongoing maintenance and monitoring procedures.

A future request for phase two will focus on modernizing technology, including replacing outdated classroom equipment and update outdated systems and software. Professional services will be used to ensure proper decommissioning of technology and replacing equipment. Finally, a future request for phase three focuses on campus safety by implementing physical security improvements and integrate communication tools for emergency response. The current system is functional but a replacement is recommended for better performance and improved efficiency.

This project is agile in the sense it is broken into standalone phases. However, the phases are not interconnected and three separate IT-related projects combined. CCA has prioritized phase one as the most critical.

Project Planning

CCA states that a thorough inventory of CCA's technology assets was conducted and revealed that 80 percent of the technology fleet was beyond their recommended lifespan. Additionally, it was found that IT staff spent most of their efforts on responding to emergency repairs and system failures rather than strategic improvements or proactive maintenance.

CCA issued a Request for Information (RFI) and worked with an approved vendor to assist in gauging the scope of the project. CCA plans to repost the RFI to allow participation of additional vendors and obtain updated pricing information. A minimum of three quotes from vendors will be required. Additionally, CCA has evaluated similar projects at other community colleges that have funded similar projects to ensure fair and competitive pricing.

The vendor will be expected to work with college IT personnel on training and capacity building for staff. It is intended that staff will be well equipped to manage the new initiatives.

The expected life expectancy for the proposed solution is three to five years for the endpoint/user devices and five to eight years for server systems and networking equipment. CCA plans to develop a sustainable lifecycle approach.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$144,000	$899,500	$49,950	$1,093,500
Software	$0	$130,975	$0	$149,850	$280,825
Equipment	$0	$676,500	$999,500	$799,200	$2,475,200
Contingency	$0	$47,525	$99,950	$0	$147,475
Total	**$0**	**$999,000**	**$1,999,000**	**$999,000**	**$3,997,000**

CCA included a 20 percent inflation rate professional services and software totals, totaling $54,450 toward the total cost for this phase alone. CCA stated that although the Higher Education Price Index forecasts a 3.7 percent inflation rate, 20 percent reflects the market pressure the institution has experienced. An example provided was the institution's current VMware license renewal cost, which has more than tripled.

Cost Benefit Analysis

CCA was not able to provide a quantified cost benefit analysis, as required by Section 24-37-304 (1)(c.5)(V), C.R.S., but notes that employees are affected by the amount of system downtime and service disruptions which impacts productivity.

Cash Funds

The cash funds will be sourced from Student Technology Fees.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	July 2026	September 2026
Design	October 2026	December 2026
Construction/Implementation	January 2027	June 2027

Staff Questions and Comments

Project Questions

Q: How was 20 percent decided on for inflation?

A: This approach incorporates feedback from vendors and accurately represents current developments in the IT industry:

Given the volatility in IT hardware, software licensing, and infrastructure costs—especially in light of global supply chain disruptions and vendor pricing escalations—this inflation factor ensures our projections remain realistic and aligned with anticipated market conditions.

While national indices such as the Higher Education Price Index (HEPI) forecast a 3.7% inflation rate for FY2025, the 20% figure used in our submission reflects the actual market pressures we are experiencing. In some cases, inflation-related cost increases have exceeded 100%. For example, our current VMware license renewal costs have more than tripled. Therefore, applying a 20% inflation assumption helps safeguard budget adequacy and prevents underfunding.

Q: How was the estimated cost for Phase 1 determined? Did you received competitive bids from any DR Consulting firms? Quotes for upgrading systems and network components?

A: We have already engaged NASPO-approved vendors and held preliminary discussions regarding the scope of Phase 1. Initially, we issued a Request for Information (RFI), and we are preparing to repost it to allow participation from additional vendors and to obtain updated pricing as part of the process.

The total amount requested for Phase 1—specifically under professional services—aligns with current market rates for this type of engagement and reflects the scale and complexity of the work involved. In our original request, the focus was on gaining a comprehensive understanding of Disaster Recovery practices, rather than on cyber security/penetration testing. For penetration testing and related cybersecurity efforts, we rely on support from the System Office (CCCS-IT) to ensure these initiatives are properly addressed. CCCS-IT manages the Security of the network perimeter and conducts regular security testing of internal systems across all colleges.

Technical Questions

Q: Has a professional consultant been chosen or have one in mind to assist with Phase 1 Strengthening Disaster Recovery Posture? If so will their experience be in state government and higher education network architecture environments?

A: CCA has not formally selected a professional consultant at this time, but CCA-IT does have one in mind. The selection will follow the RFI/RFQ process, which includes:

- Posting the opportunity through the Colorado Vendor Self Service (VSS) portal at https://vss.state.co.us/home.
    - Going out to bid for this level of service and scope of work via https://www.bidscolorado.com.
- Considering the option to hire a NASPO direct vendor, which may streamline procurement for specialized services.

The consultant under consideration is expected to support the development of CCA's Recovery Posture and ideally possess experience in state government and higher education network architecture environments, though this will be confirmed during the formal selection process.

Q: If the implementation of the Disaster Recovery/Response recommendations require purchasing or upgrading the network infrastructure by upgrading systems and network components will that also happen in Phase 1?

A: Yes. Ideally, these upgrades would be incorporated into Phase 1 of 3, as part of strengthening our Recovery Posture. We intend to follow a structured Change Management Process to ensure that any solution agreed upon and recommended by the consulting team is effectively integrated. This will also be done in close collaboration with CCCS-IT, ensuring that final

recommendations are properly supported across multiple levels of technical and operational teams

Q: Is there existing staff that is capable of managing a Cybersecurity/Disaster Recovery program?

A: While internal capacity is growing, the complexity of implementing a robust Recovery Posture may require external consulting support to guide planning, integration, and execution. This initiative will be coordinated in conjunction with CCCS-IT in order to ensure alignment with system-wide standards, leverage shared expertise, and facilitate seamless support across all levels of technical and operational infrastructure. Once an initial plan has been fully implemented and handed over to CCA-IT, the existing staff are capable of maintaining it.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Corrections

Inspector General's Offense Reporting System

Project Summary

The Colorado Department of Corrections (DOC) is requesting state funds for a new Inspector General Offense Reporting (IGOR) records database system replacement.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$510,669	$0	$0	$510,669
CF	$0	$0	$0	$0	$0
Total	**$0**	**$510,669**	**$0**	**$0**	**$510,669**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	5 of 8	Recommended for funding.

Project Status

This is the second request for funding for a single-phase project. The department submitted a similar request for FY 2025-26, which was not recommended for funding. Staff confirmed that the project is intended as a single phase and that the department does not anticipate additional capital funds requests for the project.

Project Information

Project Objective

The request is for a total IGOR records system replacement due to age and functionality of the current system, which was first implemented in 2012. DOC provided an extensive list of an Office of Information Technology (OIT) review of department technology debt, revealing that 87 percent of department systems are severely deficient ('D' or 'F' letter grade). The department received funding for different projects in FY 2023-24 and FY 2025-26, and DOC states that the IGOR system is the current top priority among the various IT needs of the department.

There are several technical deficiencies with the current system, including an inability to protect sensitive case information on the user level and inadequate reporting functionality. The department states that the new system will increase data entry capability, improve case management and review processes, and make for better compliance with state and federal law, such as the federal Victim Rights Act. Finally, DOC states that there is difficulty in receiving sufficient technical support and that the current system is not a supported platform as the OIT programmers who developed the application are no longer with the office.

Project Description

The Office of the Inspector General (OIG) is responsible for investigating criminal activity occurring within the department.[1] DOC states that the aim of the IGOR system replacement is to modernize and improve reporting, case tracking ability, and sentencing processes. According to the department, the project covers software installation and initial licensing to replace the IGOR system, as well as contract OIT developer and program manager staff to ensure integration of the new system with existing DOC databases. In addition to improved data search functionality, DOC states that the new system will offer templates for standardized forms in order to increase productivity and make efficient use of staff time. Examples of forms include affidavits, warrants, and court orders. DOC plans include agency-wide training and technical training for those directly supporting the system.

Project Planning

According to DOC, an OIT solutions engineer conducted market research of various law enforcement investigation and case management systems in use by other similar organizations in the state. The request states that the internal market research resulted in the identification of

[1] Section 17-1-103.8, C.R.S.

several viable options, both custom and off-the-shelf. The department indicates that the off-the-shelf option is the most viable due to cost.

The department will initiate a Request for Information (RFI)/Request for Proposals (RFP) process and indicates that OIT will be directly involved with an assigned developer and program manager. DOC states in response to staff questions that the developer will be engaged from the onset of the project in data identification, collection, and conversion, as well as data integration. The project manager will be an OIT resource that manages all aspects of the project. DOC also states that the RFP process will include a review of software in use by other state corrections departments.

According to DOC, there are opportunities for integration with other systems. In response to a staff inquiry concerning integration with the DeCORuM project, which has received multiple capital appropriations, the department states that it intends to integrate offender data from eOMIS (the system developed through the DeCORuM project) to create efficiencies and improve accuracy of investigative reporting. Additionally, DOC states that it anticipates similar integration opportunities with the updated human resources software, which the department received a capital funds appropriation for in FY 2023-24.

Concerning life expectancy and decommissioning, DOC reports that they expect the new system to remain viable for over 10 years and decommissioning costs will be managed through previously allocated funds.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$281,601	$0	$0	$281,601
Software	$0	$204,750	$0	$0	$204,750
Contingency	$0	$24,318	$0	$0	$24,318
Total	**$0**	**$510,669**	**$0**	**$0**	**$510,669**

Cost Benefit Analysis

While the department did not provide a full cost-benefit analysis (CBA) in the request, it states that maintaining the aging system has become cost prohibitive, due to increased OIT rates for legacy systems and servers. Further, the department anticipates significant time savings of around one hour per case file. OIG creates approximately 3,200 case files annually, saving up to 3,200 hours of work each year, equivalent to 1.5 FTE.

In a follow-up response to a request for a CBA, DOC provides a more conservative estimate of 30 minutes saved per investigation case summary. This amounts to an annual time savings of about 28 hours annually per investigator, or a total of about 1,137 staff hours. DOC goes on to state that larger, and more complex cases will generate additional time savings, allowing for more staff to focus on actual investigations, and less time spent on administrative tasks and documentation.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Design/Planning	July 2026	September 2026
Procurement	July 2026	December 2026
Integration/Installation	January 2027	April 2027
Training	April 2027	May 2027
Rollout	May 2027	N/A

Staff Questions and Comments

Project Questions

Q: On Table 1 of the request concerning tech debt, in addition to the IGOR system, the table contains the "IGOR Drug Detection Program (DDP)"; is this system impacted by the request as well?

A: This is a standalone application developed in-house for the drug detection programs for both staff and offenders. This is not currently a requirement of a new system, but will be included as a potential feature. Current plans call for OIT development of a modernized solution for the Drug Detection Program application.

Q: The Systems Integration Opportunities and Impact section mentions that agencies outside of the DOC may need to be prepared for costs related to implementation of the IGOR system. Are you able to provide more information on these costs or to quantify them? Has the DOC engaged with these agencies on this question?

A: The Department anticipates no direct costs to other agencies, simply through the implementation of a new investigations case management solution. Should a partner law enforcement agency seek out direct access or data integrations with DOC solutions, those would come at a cost to the partner agency. Current and anticipated new practice involves direct filing by OIG to the appropriate agencies for review of potential cases, which will carry no cost to any other agencies.

Technical Questions

Q: Are the options identified by the department cloud based solutions?

A: Options identified to date include cloud based and traditional on-prem solutions. The Department is open to CJIS compliant solutions of either type.

Q: Will the system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: Yes, all of these considerations have been identified and are requirements of any solution ultimately implemented. The Department consistently ensures that any vendors engaged cover these contingencies.

Q: Will the system enable logging and resolution reporting on all issues?

A: Yes, any solution will be expected to include extensive logging and audit-trails for troubleshooting and for tracking and monitoring purposes.

Q: Will the system provide proactive alerts on system events (cybersecurity)?

A: The selected solution will comply with OIT CISO standards in regards to event logs. If the solution is on-prem, the logging will be provided to OIT Security for analysis in Splunk. If the solution is cloud hosted, logging will either be monitored by OIT or the vendor.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: Yes, the system will be required to provide all of these requirements, as well as comply with CJIS requirements.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: Yes, the selected solution is anticipated to provide role-based access, based on the individual settings of each user.

Q: Will the vendor provide technical support e.g. 24/7 support?

A: Yes, any selected solution will come with robust Service Level Agreements (SLA's) regarding technical support and time requirements based on criticality of incidents.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Yes, any solution contracted will require vendors to provide top-level training and support to users.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, this will be part of any RFP conducted by the agency and factor into solution selection.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes, this will be part of any RFP conducted by the agency and factor into solution selection.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Colorado Department of Education

School Finance Modernization System

Project Summary

The Colorado Department of Education (CDE) is requesting $3,150,000 in state funds for phase two of an anticipated three-phase continuation project to procure a new school finance system.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$3,000,000	$3,150,000	$3,150,000	$0	$9,300,000
CF	$0	$0	$0	$0	$0
Total	**$3,000,000**	**$3,150,000**	**$3,150,000**	**$0**	**$9,300,000**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	2 of 8	Recommended for funding

Project Status

In FY 2025-26, the department was appropriated $3.0 million in state funding for phase one of the project after submitting a late budget request on January 2, 2025. The department is submitting this phase two request and anticipating a phase three request in FY 2027-28, each for $3.15 million. The projected total cost of the project is $9.3 million.

Project Information

Project Objective

The request replaces CDE's school finance IT system from 2012. CDE states that the current school finance system is incapable of incorporating changes to the school finance formula, including from:

- full-day kindergarten,
- the inclusion of reduced lunch in at-risk funding, and
- the English language learner (ELL) factor.

CDE notes there are three modules that are part of the school finance system: state equal, audit, and transportation. The department states that it has an existing system to support calculations, distributions and audit adjustments for school transportation funding, and that module will remain mostly unaffected by the new system. CDE states that ongoing changes to school finance have exposed deficiencies in the state equal and audit modules of the system.

According to the department, the current system requires manual population of at-risk and ELL counts into the system, and has not fully incorporated the ELL counts into audit calculations. CDE states that the new at-risk measure will also be a challenge to incorporate into the existing audit module.

According to CDE, these changes have resulted in a reliance on manual spreadsheets for calculations and manual processing for audit adjustments. CDE states that the challenges associated with incorporating these changes using the existing system create increased risk of human error. CDE confirmed that the new system would be able to accommodate modifications in the formula on an annual basis.

Project Description

Since the phase one request, the department reports that House Bill 25-1320, the most recent Public School Finance Act, adjusted calculations from the new school finance formula put in place in House Bill 24-1448, as well as extended the implementation deadline for the new formula. The departments states that both put further strain on the existing system. CDE also states that, "the need for a new system was not driven by the creation of the new formula in HB 24-1448, but the new formula certainly makes the new system even more needed."

As described in the phase one request and detailed in the Cost Information section below, the department hired consulting firm Public Knowledge (PK) to perform a comprehensive alternative analysis for modernizing the system. The recommended solution among six options is a

Modified-Off-the-Shelf (MOTS) system. It is worth noting here that the entire request amount, aside from 5 percent contingency, is for the MOTS software purchase.

The department determined the need to establish a complete timeline with major milestones including data migration and system testing. The department indicates that it plans on a phased implementation approach and is continuing to consult with PK on recommended planning objectives. With regard to staffing, the department mentions the funding for additional 1.8 FTE included as a part of passage of HB24-1448, bringing the school finance team to 3.8 FTE. The department states that manual entry will be required until the new system becomes live, as anticipated, in summer of 2027.

The department reports that without continuing funding, it will not be able to pursue software as originally intended and that it "cannot speculate on the project's feasibility with only partial funding without additional research and requests from potential vendors."

Project Planning and Procurement

CDE states that at the time of the request, there have been no funds encumbered for the project but it plans to select a vendor by the end of 2025. After the approval of phase one, CDE continued the contract with PK to support the department in gathering the required information and writing a Request for Information (RFI) and a Request for Proposals (RFP). The department shared the posted RFI as an attachment to their original submission. The RFI states that the department was gathering information from vendor organizations with experience in providing MOTS systems. In response to staff questions, CDE states that responses from the RFI indicated that the market can deliver the system the department is envisioning. Staff also inquired as to whether the department would share more information from the RFI or RFP, if requested. CDE states that it is willing to share what is available under the law. The department points out that state statute restricts sharing information about responses until an award decision.

According to CDE, the response deadline for the RFP was October 15 and the department states that it anticipates going under contract by December 1. CDE states that more details about the project budget will be available following the RFP process, and that a pricing worksheet was required as part of the RFP requirements. The department also provided additional information about the RFP in response to staff questions concerning data storage, disaster recovery, and other technical questions, which can be found in the Staff Questions and Issues section of the request.

CDE states that the anticipated lifespan of the system is seven-to-ten years before any major upgrades. CDE also states that it received a waiver from the State Purchasing and Contracts Office to have a contract for up to 15 years, including start-up time and a transition or migration

period in the event of a future system change. Concerning other states' experiences with a MOTS system, the department states that Kentucky has successfully implemented such a system at the state level, while Vermont cancelled implementation of a MOTS system due to deficiencies in functionality. CDE indicates that it will evaluate specific systems that meet the needs of the department to ensure optimal selection.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$0	$0	$0	$0
Software	$2,857,143	$3,000,000	$3,000,000	$0	$8,857,143
Contingency	$142,857	$150,000	$150,000	$0	$442,857
Total	**$3,000,000**	**$3,150,000**	**$3,150,000**	**$0**	**$9,300,000**

Cost Benefit Analysis

In response to staff questions regarding a full cost-benefit analysis, CDE pointed to the 2024 PK feasibility study. CDE had previously provided the study and is available to the committee. The study provides an analysis of six "alternatives" the department can consider for a new system, and includes a cost summary for each alternative. Initial costs for the alternatives range from between $4 and $12 million, in addition to maintaining the status quo, which has a minimal to no initial cost. Ongoing costs in the summary range from between $1 and $5 million. The study recommended the MOTS alternative, which lists an initial cost of between $5 and $9 million and ongoing costs of $1.5 and $3 million. The analysis also provides a scoring matrix between the alternatives consisting of nine factors, one of which being "costs vs. benefits". The recommended MOTS alternative scored highest on this factor and highest overall among the alternatives.

CDE goes on to state that an automated system will reduce the risk of human error and increase efficiencies as compared to the current system. The department emphasizes the stakes of ensuring accuracy and reliability in managing over $10 billion in funding distribution to school districts.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Procurement	June 2025	December 2025
Design	December 2025	August 2026
Testing	July 2026	December 2026
Training	December 2026	December 2027
Go live	June 2027	

Staff Questions and Comments

Staff Comment

CDE states in the request that it is based upon the maximum estimated cost for the recommended MOTS solution, and that out-year project costs will be updated based on the results of the RFP process. However, in responses to staff questions, CDE states that, "the department does not anticipate any significant changes to the request amount." Additionally, the departments states in responses to staff questions that, "It is anticipated that the final funding request in the FY 2027-28 budget cycle will include the final amount required and take into account the actual bid information from the RFP."

Project Questions

Q: The request indicates that, "[t]he new formula will runs [sic] concurrently with the existing school funding formula for several years." It also states that, "[t]he system will not be able to manage two funding formulas at the same time due to its lack of functionality." As the timeline for the new system as stated in the request contains a June 2027 go live date, is the department confident it will be able to perform required duties prior to the new system being in place?

A: Yes. The Department will continue to rely on manual calculations and checks to calculate the two formulas until the new system goes live in June of 2027. It is important to note that the need for a new system was not driven by the creation of the new formula in HB24-1448, but the new formula certainly makes the new system even more needed.

The current system is not able to adequately handle even small modifications to the current formula, such as the changes to all-day kindergarten, changes to the formula in SB24-188, which

included the incorporation of rural funding and a special ASCENT rate, or the changes to shift from 12 payments to 9 payments in SB24-017, also require even more manual calculations.

Q: The requests states that, "[a] more thorough understanding of Phase two of the project will be available once the RFP process has been completed." While the request indicates that outyear request amounts may be adjusted based on the RFP process, does the department anticipate any possibility of this phase two request amount being impacted by the results of the RFP?

A: Based on the comprehensive market research that was conducted prior to the request, the Department does not anticipate any significant changes from the outyear requests from the RFP process. It is anticipated that the final funding request in the FY 2027-28 budget cycle will include the final amount required and take into account the actual bid information from the RFP.

Technical Questions

Q: Data Storage- Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: Through the RFP process the Department has requested the business continuity plan from the potential vendors, which includes a written plan on how the vendor will handle disaster recovery, rollbacks, extraction, and/or eradication. This proposed plan must also include written guidance on how the vendor will handle communication with staff, CDE, school districts, and others within an emergency situation.

The Department also requested how the potential vendors will handle storage capacity and where the data storage will take place.

The Department is following all applicable RFP, Procurement, and contracting processes as outlined by state statute and the Office of the State Controller.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Yes, this was a requirement in the RFP.

Q: Will the system enable logging and resolution reporting on all issues?

A: Yes, this was a requirement in the RFP.

Q: Will the system provide proactive alerts on system events?

A: Yes, this was a requirement in the RFP.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: Yes, this was a requirement in the RFP.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: Yes, this was a requirement in the RFP.

Q: Will the vendor provide technical support e.g. 24/7 global support?

A: The vendor will be required to provide technical support, the RFP requires the vendor to maintain technical support during normal business hours, which is appropriate for the type of contract.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Training and user assistance is a requirement of the RFP. The listed requirements for trainings are below:

- Initial training for administrators, end users, and technical support staff.
- Ongoing support including a help desk, system documentation, and knowledge base.
- Optional: Embedded training content (videos, tooltips) within the application.
- Maintenance and support services to include troubleshooting, user support, and incident response during normal business hours, with emergency escalation procedures.
- Public-Facing Tools
- A simplified public dashboard or portal to view district-level funding allocations, trends, and statutory references (if required).
- Interactive tools for public stakeholders to explore how funding is calculated or allocated.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Preliminary review so far did not reveal any significant concerns with the viability of the bidding vendors. The Department has the ability during the RFP process to request financial statements to review a vendor's health and financial position in greater detail. Generally, the RFP requirements of providing references and details of their past experience indicate a vendor’s health and financial position. The Department does not traditionally request additional detailed financial documentation from vendors unless the review process reveals cause for concern.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes, this was a requirement in the RFP.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Fort Lewis College

Campus Wide Door Access Control Upgrade

Project Summary

Fort Lewis College (FLC) is requesting state funds for its Campus Wide Door Access Control Upgrade project. Funding will support replacement of existing exterior controlled access door infrastructure on the FLC campus.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$722,818	$0	$0	$722,818
CF	$389,239	$0	$0	$0	$389,239
Total	**$389,239**	**$722,818**	**$0**	**$0**	**$1,112,057**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	8 of 8	Recommended for funding.
Colorado Commission on Higher Education	8 of 10	Recommended for funding.

Project Status

This is a new, never-before-requested project that will be completed in one phase. The Joint Technology Committee did not review or recommend the previous cash funding used for this project. Due to the current vendor ending support in June 2026, FLC used cash funding to ensure interior controlled access was maintained.

Project Information

Project Objective

This project replaces controlled access doors on the FLC campus. FLC's current vendor for controlled access doors is discontinuing support for the existing controlled access platform. Without a new controlled access platform, campus security is required to manually lock and unlock exterior doors around campus. The new platform will have upgraded hardware and software to allow access for campus visitors and enhancing security of the campus.

Project Description

FLC reports that the project involves replacing existing hardware that supports door access and implementing new software for door access. 100 new electronic controlled access points will be added to all exterior doors on campus. FLC intends to start with the interior controlled access doors, followed by exterior.

The amount requested will be spent on making necessary hardware and software improvements to allow for electronic controlled access for exterior doors and professional services to make the necessary modifications to existing exterior doors. Contractors will supply labor and materials for these improvements within the amount requested.

Project Planning

FLC indicates that they have a contract with their current controlled access vendor, Transact Campus, through 2028. However, Transact Campus is discontinuing support for its own platform by June 2026. Transact Campus then vetted two partners, Genea and LenelS2, to provide a new platform. FLC reports being offered deep discounts due to this situation, and FLC is choosing Genea to provide the new platform. Transact Campus listed references for other universities it works with in a recent response to an RFI for the Colorado School of Mines.

The new platform will be cloud-based. FLC indicates that based on this fact, the new platform will be adaptable for long-term operational needs. Also based on the cloud-based model, FLC

reports that it will not be responsible for upgrades and maintenance. FLC's IT department will be responsible for the daily operations of the system and the overall operating budget impact will be absorbable within existing resources. Additionally, there is no cost to decommission the existing system.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$192,850	$661,747	$0	$0	$854,597
Software	$83,506	$0	$0	$0	$83,506
Equipment	$112,883	$0	$0	$0	$112,883
Contingency	$0	$61,071	$0	$0	$61,071
Total	**$389,239**	**$722,818**	**$0**	**$0**	**$1,112,057**

The figures in this table reflect clarification of project costs with FLC. The original submission had a small error in the cost for Professional Services, but the figures above are accurate.

Cost Benefit Analysis

FLC reports that the primary benefit of the new platform will be a reduction in campus security hours dedicated to manually locking and unlocking exterior campus doors on a daily basis. These staff could then be assigned to more critical life-safety tasks. Additionally, campus visitors and users will benefit from ease of access.

Cash Funds

FLC previously used cash funds from operating reserves to ensure the current vendor continued maintaining interior controlled access beyond June 2026.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	July 2026	August 2026
Design	September 2026	March 2027
Construction	May 2027	August 2028
Occupancy	August 2028	N/A

Staff Questions and Comments

Project Questions

Q: Is it possible to find a new vendor for the existing campus door security infrastructure?

A: It is not possible at this time to find a vendor for the existing campus door security infrastructure. Transact Campus vetted two partners for door access control, Genea and LenelS2. FLC selected the Genea platform based on cost, and suitability, and their software is cloud-based, meaning FLC does not have to perform upgrades and maintenance. Due to FLC's current contract with Transact Campus (currently through 2028), FLC was committed to one of the two partners. Deep discounts were available from each of the two partners due to Transact Campus ending their support for their own door access control system.

Q: Can you clarify the costs for this project? There is inconsistency between costs in the summary table at the beginning of the request and the narrative description of costs in the Assumptions for Calculations section. The first is that summary table includes Consultants/Contractors at $538,500, while the total for Construction and Project Costs is $583,500. The second is that cost categories in the Assumptions for Calculations section appear to include hardware that should be under the Equipment category in the summary table. Finally, the total costs under the Assumptions for Calculations section appears to be more than the total requested in the summary table.

A: It appears that the number was transposed when added to the Consultants/Contractors line in the summary table. In the summary table, the Consultants/Contractors line should read $583,500, and the installation services line below it should read $78,247. Total Professional Services should be $661,747. Total Project Costs for Consultants/Contractors should be $776,350 and Total Professional Services should be $854,597.

Technical Questions

Q: Will the new hardware replacement be made by Fort Lewis College IT Department staff or the vendor?

A: The vendor will be replacing all hardware.

Q: Was an RFP used to choose the vendor that will implement the new door access control system?

A: No, an RFP was not used to choose the vendor that will implement the new door access control system. Transact Campus vetted two partners for door access control, Genea and LenelS2. Due to FLC's current contract with Transact Campus (currently through 2028), FLC was committed to one of the two partners. Deep discounts were available from each of the two partners due to Transact Campus ending support for their own door access control system.

Q: If the ISP fails what will be the redundancy and failover mechanisms, including the capacity to run during power failures?

A: When the system is offline (temporarily disconnected from the internet) the on-campus hardware components maintain a copy of their last configuration. This means users will continue to be able to access rooms during the normal schedule. Any changes made to the door configuration, such as new users or time schedules, will not go into effect until connectivity is restored.

When a power failure occurs, most doors on campus lock automatically. Entry into a building or secure room is not possible without a physical key. For safety reasons users can always exit a building. In the event of extended power outages, staff are available to facilitate entry into a building, particularly students needing access to their residence hall.

Q: Does the vendor hold any certifications related to security and operational excellence e.g. ISO 27001, SOC 2 Type II, etc.?

A: Genea is SOC 2, Type 2 compliant. Hardware is Underwriter Laboratories (UL) certified.

Q: Will the door access control system integrate with existing security infrastructure including video surveillance and alarm systems?

A: Genea supports several integrations with video management systems and some further integrations with intercom, sensor, and emergency management platforms.

Q: Will the system enable logging and resolution reporting on all issues?

A: Audit logging on the Genea platform tracks all activity performed on the platform. This feature provides a comprehensive list of all changes made on the platform, including user activity and system events.

Q: Will the system provide proactive alerts on system events?

A: Yes, the system can be configured to send notifications when certain events occur. Notifications include:

- Your hardware controller's internet connection goes down
- Your hardware controller's battery fails
- Your hardware controller's power supply fails
- Card access denied events
- When door is held open
- When door is being forced open

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: The system supports single sign-on, two-factor authentication, and role-based access.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: Genea Access Control offers extensive customization across its interface, data handling, and business logic. Administrators can tailor dashboards, alarms, and reporting, create custom roles and attributes, and integrate with other systems via APIs, enabling granular control and automated workflows for security management.

Q: Will the vendor provide 24/7 technical support?

A: Yes, Genea provides 24/7 customer support.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Software training will be provided as setup, configuration, and operations are performed in the software. Genea also has an extensive online knowledge base.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Communications with Transact Campus confirmed that they performed a thorough process to evaluate partners that would be able to provide a scalable, maintainable, and adaptable system for long-term electronic door access needs.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar higher education settings?

A: While Genea is newer to higher education, Transact Campus, listed the following references in a recent RFI at Colorado School of Mines:

- Mercer University
- Sagrado University (In Puerto Rico)
- Touro University (private, multi-campus university)

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Front Range Community College

Cellular Systems Improvements

Project Summary

Front Range Community College (FRCC) is requesting a combination of state funds and cash fund spending authority to improve cellular coverage throughout the three FRCC campuses.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$5,468,000	$0	$0	$5,468,000
CF	$0	$356,000	$0	$0	$356,000
Total	**$0**	**$5,824,000**	**$0**	**$0**	**$5,824,000**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 10	Not recommended for funding
Colorado Commission on Higher Education	1 of 10 (tied)	Recommended for funding.

Project Status

FRCC is requesting state funds and cash funding spending authority for a single-phase project.

The project was first presented to the committee in FY2024-25 for $3.0 million, with $299,500 in requested in cash fund spending. That request was ultimately not recommended and did not receive funding. FRCC states that the cause for the increase in requested funding is due to the solution of the project initially involving an Over-the-Air technology to transmit radio frequencies. This was later determined to be less effective and reliable than their proposed solution detailed below.

Project Information

Project Objective

Currently, there are several buildings across FRCC's three campuses that have little to no cell phone coverage. The goal of this project is to install Distributed Antenna Systems (DAS) on each campus that would ensure cell phone connectivity as well as support the increasing amount of devices on the school's network.

FRCC states that it is common for students and teachers to have to exit a building to get a phone signal. Additionally, FRCC details an incident in July 2024 where smoke filled the west end of a building on the Westminster campus. While attempting to locate the source of smoke, first responders were unable to communicate with dispatch and campus security was unable to update and notify administration due to a lack of cell signal.

Project Description

FRCC states that with this funding, a third-party firm will analyze the current coverage deficiencies and design a solution. The new system will consist of the following components:

- a Central Area Node (CAN) that will digitize baseband radio frequency signals, combine the signals, and distribute them throughout a building or campus;
- a consistent, strong signal throughout 95 percent of the required coverage areas;
- a Transport Extension Node; and,
- a set of frequency-agnostic interface modules used across the wide area-integration node, CAN, and Transport Extension Node.

The system can be installed within days. All equipment will be fully supported by a manufacturer and is covered by a three-year warranty. FRCC states they will engage with a vendor via a service agreement in order to ensure a rapid response to any system failures that might occur. FRCC will be requiring a product acceptance plan, a demonstration validating design requirement, surveys validating coverage improvements, and carrier acceptance of system integrations from cellular providers.

Project Planning

In January 2025, FRCC engaged with Advanced Network Management and Engineering Wireless Services to provide an analysis and cost estimates for this project. If this project is funded, FRCC will engage with the standard Request for Quota as specified by the Office of the State Architect and state procurement guidelines.

The projected life expectancy of this proposed solution is 10 to 12 years. With the aforementioned service agreement, FRCC plans on continuous maintenance and replacement of equipment as necessary. FRCC projects this agreement will require an ongoing cost of approximately $174,000 a year.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$936,465	$0	$0	$936,465
Software	$0	$0	$0	$0	$0
Equipment	$0	$4,610,201	$0	$0	$4,610,201
Contingency	$0	$277,333	$0	$0	$277,333
Total	**$0**	**$5,824,000**	**$0**	**$0**	**$5,824,000**

Cost Benefit Analysis

FRCC was not able to quantify the anticipated efficiencies, cost-benefit analysis, return on investment, or total costs of ownership, as outlined in Section 24-37-304 (1)(c.5)(V), C.R.S., but noted the time saved by not having to exit the building for cell service as well as the increased safety.

Cash Funds

The source of cash funds for this project is college reserves.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	July 2026	August 2026
Design	September 2026	December 2026
Construction	April 2027	August 2027
Integration Testing	August 2027	October 2027

Staff Questions and Comments

Project Questions

Q: Recently, the JTC has required departments and institutions to provide quarterly progress reports, with the first report for newly appropriated projects expected following the second quarter of the fiscal year the project receives funding. Will there be any obstacle to providing updates if the project(s) receives funding this year?

A: There will be no obstacles for reporting quarterly progress.

Q: FRCC submitted the FRC IT College Wide Cellular Improvements in FY 2024-25 for a total of $2,995,000 ($2,695,500 GF and $299,500 CF). Why did the requested amount for the same project almost double in cost after just two years?

A: In 2023, the College proposed a solution utilizing Over-The-Air (OTA) RF technology to transmit radio frequencies throughout the building. Since that time, it has been determined that this approach is not the most effective or reliable method for addressing the cellular coverage challenges across FRCC campuses, due to the large amount of square feet involved (843,241 SF of State buildings and 144,196 SF of leased space). To meet the expanded coverage requirements and ensure consistent performance, a more robust and dedicated solution is needed. Along with these design changes, pricing escalations in equipment and software licensing have been anticipated since 2023, reflecting both manufacturer cost increases and broader market inflation trends.

The updated 2025 proposal incorporates an Active Distributed Antenna System (DAS) leveraging IP-based RF source acquisition technology. This enhanced design ensures both improved coverage and adequate capacity, even during periods of high network demand, preventing degradation in user performance.

The wireless carrier landscape has also evolved since 2023. Previously, FRCC could expect carriers to provide the RF signal source once the DAS was in place. However, due to shifts in carrier funding models, wireless operators are no longer supplying RF sources to enterprise customers. This responsibility has now transitioned to the building owner. As a result, the updated pricing includes the cost of the carrier-grade IP-based RF source required for the DAS to operate and meet performance standards.

Lastly, the College has gained valuable insights from the Network and IT Security Upgrade Project (2024-033123), which involved installing new Wi-Fi infrastructure throughout its buildings. Lessons learned from that project—particularly around installation logistics, coordination, and integration within existing facilities—have been applied to this proposal to ensure a smooth and efficient deployment of the cellular DAS system.

Q: Is FRCC able to quantify the anticipated efficiencies, cost-benefit analysis, return on investment, or total costs of ownership, as outlined in Section 24-37-304 (1)(c.5)(V), C.R.S.?

A: While it is difficult to quantify administrative and operating efficiencies related to having sufficient cellular signal strength to make calls from within the FRCC buildings, it is undeniable that students, faculty and staff will benefit from being able to use their phones inside the buildings.

Increased effectiveness for first responders' ability to communicate from inside buildings while handling emergencies is also hard to quantify, yet we know reducing the risk during a critical incident could save injury (or worse) for students, faculty, staff and first responders alike.

Currently due to poor cellular signal, if there is a security event, campus security personnel must step out of the building and away from their office and access to security systems and fire control panels, to communicate notifications and updates to administration and external emergency services.

Technical Questions

Q: Were there other competitive proposals submitted besides Advanced Network Management / Engineering Wireless Services, LLC?

A: ANM was engaged to help provide the equipment and budget details for the 2026/27 CCIT Proposal. Should FRCC receive funding, the College will solicit for the designer / installer as a design/build RFQ as specified by the Office of State Architect and proper State procurement guidelines. This is what was done for the Wi-Fi project.

Q: Will the cellular system improvements handle both daily traffic and peak usage during events such as sporting events?

A: YES. Although FRCC does not have sports teams, the system will be able to handle daily and peak usage. The updated technology, being an IP-based RF-source, will handle a greater number of people in our buildings.

Q: How will the new proposed system work in more difficult-to-reach buildings, i.e. thick concrete walls?

A: The proposed solution will be specifically designed to handle signals within difficult-to-reach buildings. Our Westminster Campus Building contains a large amount of concrete and 65% of the building is underground. The budget will include sufficient equipment (signal boosters/repeaters) to overcome the architectural challenges.

Q: Will the system enable logging and resolution reporting on all issues?

A: YES

Q: Will the system provide proactive alerts on system events?

A: YES. If any active component of the DAS system fails (antenna, remotes and head-end components), the system will send an alert. The system will also monitor the strength of the inbound carrier signal and alert if there is an issue.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums if the system is managed by FRCC IT staff?

A; Yes. Even though the college will enter into a maintenance agreement, the college will ensure the highest quality training is provided for FRCC IT staff where necessary. The intent of the maintenance agreement is to not burden IT staff with such maintenance duties, and it is recommended by ANM to have third party maintenance agreement for the life of system.

Q: How long do you anticipate having a service agreement with a vendor to support this system?

A: The college will maintain a service agreement that will match the duration of the licensing for the software.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar higher education settings?

A: Yes, we will ensure that the design build RFQ has that language.

Q: Would you consider inviting public safety agencies i.e. First Responders to be part of the System Acceptance Requirements by participating in the acceptance test plan?

A: Yes, the college has a close working relationship with first responders in the counties in which our campuses reside. We will ensure that the DAS system will seamlessly support their cellular-based communication equipment.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Health Care Policy and Financing

Colorado Benefits Management System

Project Summary

The Department of Health Care Policy and Financing (HCPF) is requesting state funds and federal funds spending authority to continue the re-procurement of the Colorado Benefits Management System (CBMS).

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$1,215,845	$905,237	$0	$0	$2,121,082
FF	$5,273,589	$3,918,569	$0	$0	$9,192,158
Total	**$6,489,434**	**$4,823,806**	**$0**	**$0**	**$11,313,240**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	1 of 10	Recommended for funding.

Project Status

This is a continuation request for phase three of a five-phase project to replace the CBMS system. The project was appropriated a total of $1.7 million in FY 2024-25 for phase one of the

project and $4.8 million in FY 2025-26 for phase two. HCPF indicates there will be additional capital fund requests for future phases of the project, but it is unclear as to the request amounts.

Project Information

Project Objective

Under the federal Center for Medicaid Services (CMS) and state procurement rules, the department is required to procure CBMS contracts for a maximum of ten years. Due to these requirements, the department must complete the procurement process for a CBMS vendor(s) by June 30, 2029. This project enables HCPF to follow state and federal timelines.

Additionally, federal regulations require certain modularity requirements be met in an effort to improve efficiency and effectiveness of upgrades, reduce cost, and promote interoperability. The department notes that this project is not a system replacement. Rather the department is seeking potential vendors to take over the maintenance and operation of the existing CBMS system and its two modules: Program Eligibility and Application Kit (PEAK) and Client Correspondence.

Project Description

Funding for phase one of the project was used to complete drafting requirements and hire staff to complete various research projects determining technical debt, identification of potential issues, and opportunities for modularization. Funding for phase two is currently being used to continue research and evaluation from phase one, as well as to initiate drafting the first solicitation.

The bulk of funding for this phase of the project will be used for the FTE and contractors required to continue the re-procurement efforts and ensure compliance. HCPF provided information on the cost breakdown as well as titles, descriptions, and detailed costs for the six FTE and eight contractors hired for this phase.

Project Planning

Over the next few years HCPF, the Department of Human Services (DHS), the Office of Information Technology (OIT), and stakeholders from the counties will work together to administer programs and continue to work together to create documentation on user needs, program priorities, and technical architecture in order to develop a transition strategy with the federal modularization requirements in mind.

HCPF conducted various forms of market research. The department contracted with Public Knowledge (PK), a management consulting firm, to complete a stakeholder engagement report that provided information on stakeholder feedback. Additionally, PK worked with other states and advocates to gain insight on different approaches taken, operations structures, vendor management, contracts and cost analyses, and lessons learned. They also provided a cost analysis report and an analysis of alternatives that HCPF notes as being very influential on the current direction of the project.

HCPF, DHS, and OIT are collectively working on system procurement to improve CBMS performance and usability. The procurement process will consist of Invitations to Negotiate for each module (PEAK and Client Correspondence). Additionally, the departments will work with federal counterparts, including the Centers for Medicare and Medicaid Services, Food and Nutrition Services, and the Administration for Children and Families, to meet all federal requirements.

The department states that the selected vendors will be required to deliver:

- a change management plan;
- a process to monitor, measure and control scope;
- a testing strategy;
- a training plan; and,
- operational readiness plans.

The vendors will be required to provide 24/7 technical support and to train HCPF's Staff Development Division through online curricula, videos, and desk aides. This will be the basis for additional training materials for staff and to support users.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$6,134,356	$4,589,691	$0	$0	$10,724,047
Equipment	$46,057	$4,410	$0	$0	$40,467
Contingency	$309,021	$229,705	$0	$0	$538,726
Total	**$6,489,434**	**$4,823,806**	**$0**	**$0**	**$11,313,240**

Cost Benefit Analysis

The department was unable to quantify cost savings as required by Section 24-37-304 (1)(c.5)(V), C.R.S., but notes all funding requested is necessary to comply with procurement regulations. HCPF states that partial funding would put the department at risk of losing federal financial participation.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Technical Assessment	January 2025	July 2025
Modularization and Procurement Plan	June 2025	July 2025
Staffing and Scoping for Initial Modularization	July 2025	December 2025
Procurement Process Design	July 2025	December 2025
Operational Process Design	July 2025	June 2026
Draft Procurement Documents	July 2026	December 2027
CMS Review and Approval	January 2027	March 2027
Solicitation Period	March 2027	May 2027
Evaluation Period	June 2027	December 2027

Staff Questions and Comments

Technical Questions

Q: Will the new modularized CBMS provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: Yes, all applicable requirements for storage capacity and support processes were incorporated during requirements drafting sessions.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Yes, the Enterprise System Integration team (ESI) was engaged during requirements gathering sessions to ensure their approach to integrating and all interfaces associated with the CBMS system and their related programs.

Q: Will the new modularized system support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: Yes, the system will follow the same OIT standard security process as all login requests. The requirements include role based security access. These are minimum necessary security requirements to be in compliance with our federal partners as well.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: Yes, our requirements gathering sessions included opportunities for users based on roles and security to allow for user configurable changes and a sandbox for testing changes before going into production.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, a vendor's financial health to include, but is not limited to Liquidity, Solvency and Operational Efficiency, will be considered as part of the selection process. There are also mandatory qualifications associated with personnel and additional criteria can be added based on program and system needs.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes, a vendor's reputation and past performance will be considered as part of the selection process.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Colorado Department of Health Care Policy and Financing

Social Health Information Exchange Project

Project Summary

The Department of Health Care Policy and Financing (HCPF), in partnership with Office of eHealth Innovation (OeHI), the Office of the Lieutenant Governor, and the Behavioral Health Administration (BHA) requests state funds and federal funds spending authority to continue the implementation of a social health information exchange (SHIE) system.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$2,743,279	$743,838	$0	$0	$3,487,117
FF	$16,427,714	$3,306,151	$0	$0	$19,733,865
Total	**$19,170,993**	**$4,049,989**	**$0**	**$0**	**$23,220,982**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	4 of 10	Recommended for funding.

Project Status

This is the third and final request of a three-phase continuation project. A total of $11 million was appropriated in FY 2024-25 for phase one and $8.1 million in FY 2025-26 for phase two.

Project Information

Project Objective

According to HCPF, the system will ultimately facilitate assessments and referrals to improve connecting Medicaid members to other public benefits programs, health improvement programs, and community based services. The SHIE system infrastructure is designed to be a Medicaid Enterprise System (MES) module that will bridge the gap between third-party social care platforms outside of the secure MES to other MES and state systems.

The departments state that the project may improve Coloradans' access to health care and available programs, provide important data to identify gaps between community need and available resources, and decrease the impact of social determinates of health (the non-medical factors that influence health).

Project Description

The department is using a two-pronged hub-and-spoke approach to implementation. The hub is focused on statewide data sharing and large-scale infrastructure and the spokes are focused on the needs of individual communities.

This project will focus on the following aspects over the course of the current and previous phases:

- Continue implementation and expansion of the flexible data sharing ecosystem that facilitates connectivity between SHIE users, such as Regional Accountable Entities (RAEs)/Managed Care Organizations, Colorado's Health Information Exchanges, behavioral health providers, community based organizations (CBOs), state agencies, and other organizations that deliver whole-person care.
- Implement a formal data governance structure that governs the onboarding of health improvement and social data into SHIE, and ensuring CBOs can access and utilize clinical data and send standardized referrals to clinical and non-clinical partners.
- Develop and expand an integrated consent management solution to ensure consent to share data.
- Improve the accuracy, consistency, and availability of information in a single resource directory.
- Expand regional investments.

Over the past year, the foundational architecture of CoSHIE has been built and is continuing to be developed. There are 35 users utilizing the new system along with the following five data sources:

- Department of Local Affairs Elite housing voucher data;
- Medicaid Transition to Community Request forms;
- Pre-Admission Screening and Resident Review referral source;
- Medicaid Roster; and
- 211 Community Resource Inventory with Mile High United Way.

In the next year, the system will integrate new data partners and will partner with four organizations that will assist in identifying and solving current barriers.

Through Senate Bill 21-286, HCPF applied for and received $15 million in funding through the American Rescue Plan Act and Home Community Based Services Cash Fund to initiate the development of SHIE, formerly known as Prescriber Phase II. That funding expired September 30, 2024, and the department has successfully completed the creation of Prescriber Phase I, the Opioid Module and Affordability Modules, which are currently operational.

According to the partnership agencies, without this funding, the project would stall and remain at the base-level development. Colorado is the first state to have approval from the Centers for Medicare and Medicaid Services (CMS) to build SHIE within a state's MES framework, giving Colorado the opportunity to lead the nation in leveraging technology to improve health improvement services and social care services.

Project Planning

HCPF, in conjunction with BHA, DHS, Colorado Department of Public Health and Environment (CDPHE), Colorado Department of Corrections (DOC), local public health agencies, CBOs, and other stakeholders have worked together to over the course of years to identify successes, lessons learned, and ways to avoid duplicative efforts.

The aforementioned state agencies in conjunction with the Office of Information Technology have been highly involved with the procurement process. During the development phase for the Invitation to Negotiate, HCPF conducted extensive market research, including interviews with RAEs, local governments and CBOs. Additionally, HCPF reviewed North Carolina's NCCARE360, San Diego's Connect Well SD, and Washington State's Community Information Exchange to identify best practices and lessons learned.

The selected vendor displayed alignment on the desired system architecture, scalability, interoperability, and the ability to support integration across CBOs, health care providers, and public programs.

While HCPF has their internal change management process, all vendors will be required to deliver a change management plan that includes a scope control process, process to monitor and measure scope, testing strategy, training plan, and operational readiness plans.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$18,208,002	$3,853,089	$0	$0	$22,061,091
Equipment	$50,086	$4,043	$0	$0	$54,129
Contingency	$912,905	$192,857	$0	$0	$1,105,762
Total	**$19,170,993**	**$4,049,989**	**$0**	**$0**	**$23,220,982**

Cost Benefit Analysis

The department was unable to quantify cost savings as required by Section 24-37-304 (1)(c.5)(V), C.R.S., but noted that complex case management, which will be a Medicaid program associated with SHIE, helps better support the 4 percent of Medicaid members who consume 40 percent of Medicaid spending. The system will connect members to care coordination and the complex case management will have a direct increase in program utilization, savings, and better outcomes.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Planning and Discovery	November 2023	February 2024
Design, Development, and Implementation	March 2024	March 2027
Maintenance and Operations	April 2027	June 2033
Implementation of Regional Proofs of Concept	July 2025	June 2028

Consent Management Proof of Concept	March 2024	December 2025

Staff Questions and Comments

Project Questions

Q: Have the community organizations that will help identify and solve potential barriers to the system already been chosen and have agreed to be on board with the project?

A: Yes, the state has chosen 4 community organizations. Each organization has a signed and executed contract with the state and have begun working with the project team since the beginning of the 2025/26 state fiscal year.

Technical Questions

Q: Was the vendor that participated in the ITN process experienced with CoSHIE type systems in other states?

A: Colorado is pioneering the sharing of Social Health information and therefore a system similar to CoSHIE does not currently exist. However, at its core, CoSHIE is a platform for data sharing. Based on this foundation, yes, the vendor does have experience with developing data sharing systems in several other states.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, as part of the ITN, some sections mandate certification regarding debarment, suspension and disclosure of past financial or contractual problems. These disclosures are then reviewed during the evaluation process for the ITN.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: No specific references were provided with their application. However, they did provide several different state agencies they worked with along with descriptions of the projects.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Colorado Department of Labor and Employment

CoCo System Replacement

Project Summary

The Department of Labor and Employment (CDLE) is requesting cash fund spending authority to replace the workers' compensation computer system and database, commonly known as CoCo[1].

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CF	$20,767,026	$9,964,519	$0	$0	$30,731,545
Total	**$20,767,026**	**$9,964,519**	**$0**	**$0**	**$30,731,545**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	3 of 3	Recommended for funding.

Project Status

This request is for phase three of a three-phase project to replace the CoCo data system. To date, the department has received $20.8 million in cash fund spending authority from the Workers' Compensation Cash Fund, Subsequent Injury Fund, and Major Medical Insurance Fund ($8.6 million in FY 2024-25 and $12.1 million in FY 2025-26).

[1] The project is also referred to as CoComp.

Project Information

Project Objective

The project will create a system that integrates all workers' compensation workflows and processes, and provide the ability to file all forms electronically. According to the department, this allows for increased accuracy, efficiency, and improved user access by staff as well as external stakeholders such as insurance carriers, medical providers, attorneys, and injured workers.

Project Description

The current CoCo system operates as a database with limited workflow, causing several work units to create separate, non-state-supported external systems to accommodate their workflow. The new system will provide user controlled access and eliminate employee designed systems and current risks associated with potentially high-risk email form submissions vulnerable to phishing and malware.

Through the first and second phases of funding, CDLE has completed the discovery phase of the project, finding pain points of the current system and ways the new system can be improved. After a lengthy procurement process, the department selected vendor CapTech for the new system. In addition, the discovery and data assessment phases have been completed, and the product backlog has been defined. Currently, the development sprints are being completed.

Phase three of the project will be dedicated to final launches of systems, testing, and troubleshooting. The system will go live internally while CDLE and the vendor work through fixes before releasing the system to stakeholders. The vendor is expected to provide post-implementation maintenance and training. Afterwards, OIT will be responsible for all support responsibilities.

Although CDLE did not provide the most recent quarterly update, they have previously reported the project on time and within budget.

Project Planning

In 2018, CDLE met a state mandate to transition off of a legacy system, but the system was not fully modernized. As a result of the pandemic in 2020, CDLE was required to build unsustainable short-term solutions that were not supported by the Office of Information Technology.

CDLE conducted an Invitation to Negotiate (ITN), requiring potential vendors to complete a task or presentation displaying workflows and screen mockups of the proposed solution. 11 vendors

submitted proposals and were fully engaged. CDLE then narrowed the pool down to five vendors who presented revised proposals. The selected vendor, CapTech, has successfully implemented projects in 13 other states and is a Statewide Internet Portal Authority (SIPA) vendor. CDLE held meetings with a handful of these states to review pros and cons ultimately decided this was the best fit. Detailed descriptions of CapTech being used in other states is provided in the "Staff Questions and Issues" section of this request.

While transitioning to the new system, the old system will be working in tandem to prevent any disruptions in service. CDLE will be utilizing the vendor for the implementation of the system and states the first release of the system will not include stakeholders to allow continuous improvements be made. CDLE will then provide training, assistance, and support through the call center for stakeholders as the new system is made available. CDLE projects the system will be viable for ten to fifteen years and will cost between $84,000 and $95,000 to decommission the old system based on the salaries of the OIT resources over an estimated duration of two months.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$2,429,114	$1,058,654	$0	$0	$3,487,768
Software	$16,000,000	$8,000,000	$0	$0	$24,000,000
Equipment	$450,000	$0	$0	$0	$450,000
Contingency	$1,887,911	$905,865	$0	$0	$2,793,776
Total	**$20,767,025**	**$9,964,519**	**$0**	**$0**	**$30,731,544**

Cost Benefit Analysis

The department was unable to quantify cost savings as required by Section 24-37-304 (1)(c.5)(V), C.R.S., but noted cost savings due to an increase in efficiency and decrease in error requiring duplicate efforts.

Cash Funds

The cash funding will be sources from the Workers' Compensation Cash Fund, Subsequent Injury Fund, and Major Medical Insurance Fund.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
External Portals Planning and Development	April 2026	August 2027
Internal Portal Cutover and Go-Live	June 2026	July 2027
End-to-End UAT Testing	August 2026	September 2027
External Portals Planning and Development	April 2026	August 2027
Internal Portal Cutover and Go-Live	June 2026	July 2027
External Portal Cutover and Go-Live	September 2027	November 2027

Staff Questions and Issues

Q: On the first page of the request, it is stated there were delays in procurement. Please provide more details as to why the procurement was delayed. Did this impact the cost of the project? What safeguards were put in place before and after?

A: Procurement delays were the result of technology platform decisions involving the Division, the Vendor, and OIT. There were a significant number of discussions as the requested and documented architectural platform was not accommodated by OIT. The decision was eventually made to revise the architectural requirements to allow for the Amazon Web Services platform. These ongoing discussions not only affected the timeline but also required additional setup costs that had to be drawn from the project budget, which was not originally accounted for. At the same time, OIT was updating their project oversight process, which resulted in delays relating to responsibilities, resources, leadership, and the approval processes.

Q: In the Background Information section on page 2, it mentions other states' successes and failures. What have you learned from other states that you are incorporating or avoiding?

A: The awarded vendor, CapTech, has successfully implemented projects in 13 other states. Initial discussions were held with a select number of these states to gauge the pros and cons of their vendor experiences. DOWC has selected Information Technology Values that are monitored across each phase of this replacement project, which have been successfully implemented globally in other state projects. These include the following:

- Integration - Is the solution integrated into the larger system?
- Cost Avoidance
- User Productivity

- Risk Reduction
- Accessibility
- Stakeholder Impact
- Delivery of Service Impact
- Operational Rating - Essential (0-30 Days), Critical (31-60 Days), Non-Critical (61+ Days)
- Sustainable Maintenance Requirements.

Q: Is there an estimated amount of technical debt that is accruing as mentioned in the procurement section?

A: It is anticipated that there will not be accrued technical debt within our replacement system. This project is eliminating approximately 10 years of technical debt, spanning multiple applications and hardware that will be decommissioned upon the new application's final release in the Fall of 2027, with vendor warranty extended through early 2028.

Q: It is mentioned the estimated annual maintenance for the new system will be $100k. What is the breakdown of that cost? What is the annual licensing fee for this option?

A: Initial estimates of $100k for system licensing were provided based upon past application trending costs and prior to our obtaining a State-awarded contract with CapTech. This number is expected to change, but cannot be accurately estimated at the moment, as decisions on tools and software are still being made. The initial plan is to continue engaging with our OIT partners to ensure that maintenance is performed proactively on an annual basis. Given that the final product is not expected to go live until late 2027, it is impossible to predict that number. This also applies to the annual licensing fees; however, as the Division gains a better understanding of the final software decisions, this number will become easier to document.

Please note, once this new system is in production, we will no longer be dependent on a vendor for ongoing support. This product will be wholly owned by DOWC and supported by OIT and therefore we anticipate lower maintenance cost.

Q: Is there a plan to transfer data from the existing CoComp database to the new system, if so, how many years of data will be transferred?

A: Yes, through a collaborative (OIT and CDLE) data management policy, we are transferring not only the entirety of the existing CoCo Database, but also critical data that exists in ancillary databases, to the new system. While a final determination on the number of years of data that will be migrated has not been decided, the discussion is ongoing.

Q: Now that OIT's master contract for the licensing of Maxenso is no longer in place, can that system be recovered today if DOWC experienced a disaster that affected that server that hosts DOWC (Maxenso)?

A: Yes, a full database and application recovery is available if needed.

Q: Is the Maxenso system being backed up on a daily basis and archiving data at this time?

A: Yes, the current Maxenso Enterprise Engine application, along with the Primary SQL database, is backed up nightly at 2 AM. The actual database is backed up nightly at 11 PM.

Q: What is the anticipated type of technology that will replace the PDF forms that are currently being received by the DOWC widely published email in box?

A: Current form processes will be replaced with automated workflows and include online digital forms, replacing PDF's for the remaining information that needs to be collected.

Q: Are the workflows in the full system replacement option new, or are you anticipating implementing the existing workflows into the new system, if so, will they be efficient?

A: Yes, all of the existing workflows are in the process of being modified to accommodate modernization efforts pertaining to this project. To maximize efficiencies within DOWC, we reviewed each of our system workflows with Government Performance Solutions (GPS) prior to awarding CapTech the contract and during requirements gathering, all of the workflows were further reviewed by our vendor, Captech, to ensure appropriate user stories for applicable development.

Q: Data Storage- Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: Yes, all of the above functionality exists within the Amazon Web Services platform, providing highly scalable and elastic storage capacity as well as diverse data types and strategies for data protection and management.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Yes, assumptions regarding relevance include the enterprise applications and service offerings that currently interact within the existing enterprise domain.

Q: Will the system enable logging and resolution reporting on all issues?

A: Yes, in accordance with OIT Service Level Agreements.

Q: Will the system provide proactive alerts on system events?

A: Yes, in accordance with OIT Service Level Agreements.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: Yes, in accordance with practicing OIT security Policies and Procedures.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: Yes, The System is utilizing modernized development tools and technologies, enabling system customization with ownership of the source code belonging to DOWC.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Yes, in accordance with the existing contract. Training, assistance, and user aids will be developed and executed in a phased approach as external stakeholders will not have access to any of our systems during the first release. Prior to go-live, the Division will hold multiple stakeholder meetings to inform the overall needs and design of the internal and external interfacing portions of the system. Additionally, the vendor and Division will jointly host multiple webinars and live training sessions, develop job aids, and provide support through our call center to assist in training stakeholders on the use of the new system.

Q: Will some research be done on the vendor health, e.g., is the vendor in a strong financial position?

A: CapTech is a SIPA vendor, and CDLE has worked with them on other projects, e.g., accessibility testing. Between the SIPA vetting process and the discussions with other states, the Division was comfortable moving forward with the chosen vendor. However, CDLE has plans to strengthen our procurement process to include vendor health as part of the vendor selection process.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: The Vendor provided several references for working on similar projects with other states and government organizations.

Minnesota Department of Labor & Industry - August 2018 – February 2023

CapTech successfully replaced an outdated internal-only document-based system that had been in use for over 25 years. The legacy system could no longer be maintained or enhanced and failed to meet the electronic access expectations of its stakeholders. CapTech undertook a comprehensive approach, including assessment, business process re-engineering, project management, development, testing, and deployment to deliver a modern, efficient, and user-

friendly solution. CapTech implemented a new data-focused web portal designed to serve both internal and external user needs.

Kansas Department of Labor - January 2017 – November 2018

CapTech deployed a modern workers' compensation platform that serves the entire lifecycle process. This new platform features include Electronic Data Interchange (EDI), claims management, dispute resolution, fraud detection, payment processing, proof of coverage, medical fee management, and various forms.

Virginia Department of Criminal Justice Services - April 2022 – February 2023

CapTech partnered with Virginia DCJS to deliver a modern, custom case management system built from the existing case management platform to track services provided to victims of crime in the Commonwealth of Virginia. The new solution replaced a egacy system that had become inadequate in providing efficient services to the growing candidate base. CapTech worked to modernize business processes and allow the platform tools to automate tasks, resulting in cleaner data, more accurate case data, and faster service times to crime victi

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Otero College

Campus Security Upgrades

Project Summary

Otero College (OC) is requesting state funds and cash fund spending authority for a replacement of 90 aging security cameras and upgrading 25 point-to-point camera connections to hardline connections for its campus surveillance system.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$184,300	$0	$0	$0
CF	$0	$50,000	$0	$0	$0
Total	**$0**	**$234,300**	**$0**	**$0**	**$0**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Colorado Commission on Higher Education	1 of 10 (tied)	Recommended for funding.

Project Status

The request is for a single-phase project. In FY 2025-26, OC requested roughly $500,000 in state funds to upgrade security cameras, as well as replace laptops. The laptops portion made up $315,000 of the total request amount. The committee did not recommend funding the request. The college made a similar request for both software and equipment upgrades in FY 2024-25, which was also not recommend for funding.

Project Information

Project Objective

OC states that the project objective is to replace an aging security camera system with new equipment and upgrade connection technology for a specified number of cameras on campus. OC indicates that the existing 25 wireless camera connections to be replaced with hardline connections are outdated and unreliable. The college also states that the existing cameras are 13 years old and video footage is of low quality. In addition, OC states that new cameras will enable gun detection technology, which would improve physical safety of the students in the event of a security incident on campus.

According to OC, that the replacement would enable the college to better prevent and respond to cyber-security threats, and that hardwired infrastructure provides increased reliability and security for the system. According to the college, transmission of video data, improved data storage, ability to better recover from cyber incidents, and improved monitoring of the college's IT assets all contribute to improved cyber security. OC reports that there will need to be future upgrades to existing cameras not included in the request; however, the college did not provide details of when this might be required. The college does include future IT capital needs in its 5-year plan, which does not include additional security camera upgrades.

Project Description

OC intends to initiate the project in a pre-design phase once funds are appropriated. The college plans to begin a procurement process soon after, with vendor selection planned in the fall of 2026. When asked by staff about vendor selection, OC states that it will manage a competitive Invitation for Bid process and purchases will utilize state price agreements where applicable. The college plans to follow a structured procurement process in accordance with state requirements. OC plans to complete the install component of the project by the summer of 2027. According to the college, the new cameras will integrate into the existing security system.

OC indicates that equipment costs in the request were determined through assessing current market value and that the college will be able to accommodate any discrepancies in actual costs using other funds to ensure project completion.

Project Planning

OC discussed its project management approach. The college intends on protecting the value of the investment by continually tracking and assessing the condition of the new security equipment. Equipment details will be documented in a central asset management system to manage lifecycle planning. The college states that it plans to hold regular progress meetings to monitor milestones, address emerging issues, and ensure accountability among stakeholders. OC states that much of the upgrade implementation will occur with minimal disruption to day-to-day activity of campus users.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Equipment	$0	$234,300	$0	$0	$234,300
Total	**$0**	**$234,300**	**$0**	**$0**	**$234,300**

Cost Benefit Analysis

The college was not able to provide a complete cost-benefit analysis. However, it did provide some operational savings projections, including IT staff saving one-to-three hours per day resulting from better performance of new equipment. OC also emphasized improved reliability, thus reducing the risk of emergency repairs and savings from avoiding high maintenance costs associated with legacy systems.

Cash Funds

The request includes $50,000 in cash funds. The Colorado Department of Higher Education applies scoring criteria in order to rank projects. One factor in the criteria is contribution of other funding sources. However, certain institutions, including OC, are exempt from this criterion. As such, contribution of cash funds does not affect scoring.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	July 2026	July 2026
Design	August 2026	August 2026
Procurement and vendor selection	September 2026	November 2026
Installation	November 2026	June 2027

Staff Questions and Comments

Staff comment

Joint Rule 45 states that the JTC shall review budget requests exceeding $500,000. This request is for less than this threshold. However, considering the background of the request described in Project Status section above, staff feels that it seems reasonable to consider the request through standard evaluation and prioritization by the committee.

Project questions

Q: How was the 25% risk factor calculated*?*

A: The 25% risk factor represents the estimated probability that significant risks, such as system failure or security incidents, could occur if the project is not funded. This estimate is based on current system unreliability, age of equipment (nearly 13 years old), vulnerabilities inherent in the existing wireless connections, and historical incidents impacting surveillance effectiveness.

Q: In Section D. PROGRAM INFORMATION: It states that the College IT staff will collaborate with a trusted local cable installation contractor, and the college will partner with multiple vendors to ensure a seamless and efficient process. Will there be a competitive RFP to choose these vendors, or is equipment being purchased using state price agreements?

A: The College will select installation contractors through a competitive Invitation for Bid (IFB) process to ensure transparency and quality. Equipment purchases will utilize state price agreements where applicable, maintaining compliance while achieving cost efficiency.

Technical Questions

Q: Will the video footage data from the new cameras be on existing servers or in the cloud?

A: All current and future camera footage will be stored on the College's local servers and subsequently backed up to the cloud. This approach ensures secure and reliable access while maintaining data protection through backup and disaster recovery measures.

Q: Will there be or is there a current policy in place for video data storage? Example:

- Minimum Retention
- Security- Data stored in a secure controlled location limited to authorized personnel
- Data Access- Access to footage is restricted
- Purpose and Privacy- Surveillance is primarily for crime deterrence and investigation
- Extended Storage- under certain conditions data footage can be kept longer than your standard policy set?

A: Yes, the College maintains a comprehensive policy for video data storage, including:

- Minimum retention periods – 90 days for all footage
- Security- Data stored in a secure controlled location limited to authorized personnel – All campus doors are secured using our SMS access control system.
- Data Access – Access to footage is restricted – Only cabinet approved personnel have access to our security camera system.
- Purpose and Privacy – Surveillance is primarily for crime deterrence and investigation. – Surveillance is primarily intended to deter criminal activity and support investigations, while ensuring compliance with privacy standards and protecting individual rights.
- Extended Storage- under certain conditions data footage can be kept longer than your standard policy set? – This can be done by our security team if required.

Q: Will the system enable logging and resolution reporting on all issues (cybersecurity)?

A: Yes, the current system logs all user sessions, and the upgraded system will maintain this capability. It will also allow the College to track any security problems and make sure they are properly addressed.

Q: Will the new video system provide proactive alerts on system events?

A: The current system is capable of basic notifications. Additionally, the College's security team actively monitors camera failures, connectivity issues, and other system events to ensure timely response and overall system reliability.

Q: Will the new video System support user authentication, password policy management, two-factor authorization, single sign-on and role-based access?

A: Yes, the new video system will support user authentication, enforce password policies, enable two-factor authentication, allow single sign-on, and provide role-based access controls to ensure secure and authorized system use.

Q: Will the vendor provide technical support e.g. 24/7 tech support?

A: Yes, the vendor will provide technical support, including 24/7 assistance, ensuring timely resolution of issues and continuous operation of the video system.

Q: Will the vendor provide best-in-class training and assistance for users using the video system?

A: No additional training will be necessary, as all new cameras will fully integrate into the existing system. Users will continue operating the system as they do currently, with no changes to workflow.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, as part of the IFB process, the College conducts due diligence on all vendors, including reviewing financial stability and overall business health, to ensure they can fulfill contract obligations and provide ongoing support.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes, as part of the vendor selection process, the College will require all prospective vendors to provide a minimum of two high-quality references from organizations in similar government or institutional settings. These references will be carefully reviewed to ensure the vendor has a proven track record of delivering reliable, high-quality services and equipment in comparable environments.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Personnel and Administration

Statewide Procurement System

Project Summary

The Department of Personnel and Administration (DPA) is requesting cash fund spending authority for phase two of a two-phase request to procure and implement a centralized procurement system.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$0	$0	$0	$0
CF	$1,420,957	$2,299,500	$0	$0	$3,720,457
Total	**$1,420,957**	**$2,299,500**	**$0**	**$0**	**$3,720,457**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	2 of 3	Recommended for funding from cash funds.

Project Status

This is phase two of a continuation project. The department was appropriated $1.4 million from the Supplier Database Cash Fund in FY 2025-26 for phase one of the project.

Project Objective

This project aims to replace Colorado's current decentralized eProcurement system with a centralized statewide solution. According to DPA, the project involves a complete inventory of the state's existing procurement systems, identifying and implementing a new system, and integrating existing systems as necessary. The department states that the current fragmented system includes the use of the following disparate platforms:

- CORE;
- Contract Management System (CMS);
- SPCO eSubmission system;
- State Price Agreement Website;
- Rocky Mountain BidNet;
- Box.com;
- Salesforce;
- eClearance; and,
- various agency-developed tools.

DPA states that the primary deficiency of the current system is duplicative processes, which results in increased costs. Additional issues include the inability to generate meaningful analytics, limited data sharing for purchasing patterns, spend tracking, and interference in bulk purchasing capabilities. Further, the department indicates that a new system will better enable it to manage the Statewide Supplier Diversity program, which requires robust data to implement essential changes, such as facilitating certification documentation and publicly announcing upcoming solicitations to enhance vendor preparedness.

Project Description

DPA states that the project encompasses identifying existing eProcurement systems in the state, conducting a thorough processes and systems analysis, implementing a new centralized system, and integrating existing systems. Project requirements include the replacement or significant upgrade of the existing Contract Management System (CMS), a statutorily required system for monitoring all state personal services contracts.[1] Other requirements include innovative "Amazon-style" cart capabilities for price agreements and capability of conducting full e-submission requests, among others.

DPA states that phase one enabled the department to hire a dedicated product owner. Staff inquired about additional details and DPA reported that the product owner term coincides with

[1] Section 24-106-103, C.R.S.

the expected deployment of the system. DPA also states it is finalizing the process of contracting with a vendor to conduct a market scan and roadmap development.

Phase two will implement the new IT solution. Phase two will focus on soliciting and contracting with system vendors, followed by implementation and integration.

Project Planning

According to the department, the currently underway phase one includes the internal review of existing systems and much of the procurement process. DPA plans to complete phase one by June 2026. The department indicated in a response to staff questions that the project is currently on-track and within budget. The department plans on integrating existing disparate applications with a new centralized procurement system, the selection of which is expected by November 2026. DPA was not able to provide system lifespan or contract length for the new system when asked by staff.

Throughout both phases, DPA states that the project employs agile methodology with iterative "sprint cycles", which aims to minimize implementation risk. DPA insists that this approach will enable rapid delivery of usable software functionality to users. The agile framework also supports effective change management by allowing for continuous feedback and adjustment throughout the implementation process. The department states that the change management plans incorporate a standard governance model, involving both executive and end-user workgroups.

DPA states that detailed market research will include the experience of other similar state systems to help guide the department's procurement approach. Additionally, the outcomes of the comprehensive study are designed to provide the department with insights into managing disaster recovery within eProcurement systems.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$1,344,272	$1,168,000	$0	$0	$2,512,272
Software	$0	$1,022,000	$0	$0	$1,022,000

Equipment	$9,020	$0	$0	$0	$9,020
Contingency	$67,665	$109,500	$0	$0	$177,165
Total	**$1,420,957**	**$2,299,500**	**$0**	**$0**	**$3,720,457**

Cost Benefit Analysis

While the department reported the project scope includes a comprehensive business process analysis, which will enable DPA to identify inefficiencies and address existing redundancies, it did not provide a full cost-benefit analysis (CBA). In a response to a follow-up question from staff, DPA indicated that the department is in the process of developing a comprehensive CBA and total cost of ownership. DPA states that efficiencies will be realized from consolidating multiple systems workflows, streamlined solicitation, evaluation and contract management through centralized data, and integration with CORE.

According to the department, it intends on delivering a formal CBA and return on investment analysis in the future. DPA states that the new system will incur annual costs for other state agencies and departments, which will be managed under a common policy. It further states that some of these costs may be partially offset by the decommissioning of CMS, which has its own usage fees. The department plans for ongoing licensing, support, and staffing costs, which may affect its operating budget.

Cash Funds

The source of the cash funds is the Supplier Database Fund, which generates revenue through a one percent rebate on State Price Agreement total spend.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Development & Planning	May 2025	June 2026
Vendor contracting	July 2026	November 2026
Implementation	November 2026	July 2027

Staff Questions and Comments

Project Questions

Q: Can you provide some more detail on the role of the Office of State Controller in both phases of the project?

A: The Office of the State Controller (OSC) serves as a key governance and oversight partner for the eProcurement Modernization Project. Because the new system will need to integrate with CORE - the State's financial system managed by the OSC - their team plays a critical role in ensuring alignment with statewide fiscal policies, data standards, and reporting requirements.

During phase one (Planning), OSC contributed to discussions regarding system integration needs, data governance, and the transition strategy from legacy tools such as the Contract Management System (CMS), CORE's Vendor Self Service (VSS), and Perceptive modules.

In phase two (Requirements and Solution Definition), OSC continues to provide input on accounting and contract reporting requirements, approval workflows, and fiscal compliance touchpoints that must be maintained in the future solution. Their participation ensures that any new procurement platform will complement - rather than duplicate - financial processes managed through CORE and CMS.

As the project progresses toward solicitation and implementation, OSC will remain an active partner in design validation and testing to confirm end-to-end system compatibility and compliance with statewide financial policies.

Q: The narrative states in the Proposed Solution section that phase two funds will be used for, "consulting costs for a feasibility study, market scan, roadmap development". However, the project time table indicates that this is part of the phase one appropriation. Will the phase two funds be for only system vendor contracting and implementation costs?

A: Phase two funding will be used for development and implementation costs of the new system

Q: Will posting/advertising the RFP/RFI/RFQ/ITN be part of the new e-procurement system?

A: Yes, posting and advertising state solicitations (e.g. REP, RFI, RFQ, and ITNs) will be part of the new e-procurement system.

Technical Questions

Q: Will the new centralized eProcurement system be cloud based?

A: The system is intended to be cloud-based.

Q: Will the data be migrated from each current desperate system into the new system?

A: Data discovery and discussions regarding data migration are underway.

Q: Data Storage- Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: The Department has not selected a new procurement system but the Department expects that the future system will have ample storage capacity and will comply with all OIT disaster recovery requirements and standards.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: The Department has not selected a new procurement system but the Department expects that the future system will support all OIT user authentication requirements and standards.

Q: Will the vendor provide technical support e.g. 24/7?

A: The Department has not selected a new procurement system but the Department expects that the future system vendor will provide 24/7 technical support.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: The Department has not selected a new procurement system but the Department expects that the future system vendor will provide best-in-class training and assistance for users.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: As part of the sourcing process, vendor health will be verified to ensure the vendor is in a strong financial position.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: The Department will require at least two high quality references in similar government settings for the pending solution.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Personnel and Administration

Statewide Human Resources Information System

Project Summary

The Department of Personnel and Administration (DPA) is requesting state funds for its new Statewide Human Resources Information System (HRIS) project. The HRIS project will replace fragmented human resources (HR) systems and functions across state agencies with a single system.

Table 1

Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$955,500	$13,340,574	$50,335,548	$64,631,622
CF	$0	$0	$0	$0	$0
Total	**$0**	**$955,500**	**$13,340,574**	**$50,335,548**	**$64,631,622**

Table 2

Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	6 of 8	Recommended for funding.

Project Status

This is the second request for funding a new HRIS project; however, DPA has requested and received funds for similar projects since FY 2014-15. DPA requested funding for phase one of

this project in FY 2025-26, but was not recommended for funding and did not receive an appropriation.

DPA and the Governor's Office of Information Technology (OIT) were appropriated a total of $41.6 million in state funding from FY 2014-15 through FY 2019-20 for the Human Resource Information System (HRIS)/HRWorks project, which was intended to replace the state's existing payroll system and to eliminate or consolidate existing agency human resources systems. In December 2019, DPA requested an additional $12.4 million in state funding to continue working on the project using an agile methodology. However, due to the COVID-19-related budget cuts made by the General Assembly in 2020, DPA did not receive this additional funding for the HRWorks project and the project was terminated. No useable new systems were implemented with the state funding. There is a now a current project for a payroll system (DPA Payroll Management) separate from this HRIS request with appropriations approaching $51.1 million.

Project Information

Project Objective

This project will replace the existing, fragmented systems used by state agencies for various HR functions with a single platform. Currently, state agencies must utilize these fragmented systems for each HR function workflow, with some functions also dependent on paper-based solutions. Advanced HR functions, such as succession planning, are not supported with current systems. The proposed solution of the HRIS project is to create a unified software-as-a-service (SaaS) platform for state agencies to use in their HR workflows.

The proposed capabilities of this new system will include reporting and analytics; human resources (HR) process and file management, talent management, applicant tracking, workforce management; and employee relations. This system will not include HR functions such as payroll, time and leave, benefits administration, learning management, risk management, and workers' compensation.

Project Description

Phase one will fund a study for the project. The funding will support the hiring of a three-year term-limited product owner within the department to oversee the project and engage a Human Capital Management Procurement Consultant for use-case development and vendor evaluation

The department plans to use an agile approach, but indicates that more information about future phases of this project, functionality of the system, and contingency plans will be available after completing the study.

Project Planning

This request is essentially funding to support a comprehensive project planning phase prior to initiating the project, which the department indicates is necessary for the complexity of the proposed project. The department states it will incorporate the following into the procurement process:

- engaging with the aforementioned procurement consultant to identify requirements and ensure they are of focus for vendors;
- draft procurement documents with consultation of the OIT;
- facilitate vendor evaluations, testing, and selection with the participation of OIT and subject matter experts;
- negotiate a contract with the assistance of OIT verifying all requirements are met.

Throughout the procurement process, the department will incorporate input from agency customers throughout the later stages of procurement.

At this time, the department expects a 30-year lifecycle for the new system based on the use of a SaaS model. More information about project planning is expected after the study is completed.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$900,000	$3,497,308	$10,094,617	$14,491,925
Software	$0	$0	$9,198,000	$37,814,000	$47,012,000
Equipment	$0	$10,000	$10,000	$30,000	$50,000
Contingency	$0	$45,500	$635,265	$2,396,931	$3,077,697
Total	**$0**	**$955,500**	**$13,340,573**	**$50,335,548**	**$64,631,622**

Cost Benefit Analysis

The department expects significant efficiencies from implementation of the HRIS project, but a full cost-benefit analysis is not available at this time. The study funded by phase one will help create a full cost-benefit analysis.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Hire Product Owner	May 2026	July 2026
Gather Requirements	August 2026	December 2026
Fit Gap Analysis	August 2026	December 2026
Draft Procurement	November 2026	February 2027
Solicitation and Contracting	March 2027	April 2028
Implementation Phase 1	May 2028	June 2029
Implementation Phase 2	July 2029	June 2030
Testing	July 2030	September 2030
Go Live	October 2030	March 2031
Post Go Live Support	April 2031	May 2031
Continuous Product Improvement	June 2031	Ongoing

Staff Questions and Comments

Staff Comments

Based on previous work conducted by the department and other stakeholders, possible research from other states, and lessons learned from the state's other large IT systems, there may be existing knowledge within the department or OIT to identify viable solutions for a statewide HRIS.

Project Questions

Q: Are any other funds or resources available to complete the study? Why is funding for a study needed?

A: The department has not been able to identify any other funding sources for this study. Funding for the study is needed to evaluate options for implementing the first statewide HRIS. The study will include an updated analysis of current systems, assessing their capabilities and identifying how they can be leveraged or replaced to comprehensively address strategic priorities.

Q: Can you provide more detail on mitigating the risks of implementation? Will other state agencies need funding for implementation? What will happen to the legacy systems and processes they are currently using?

A: Upon completion of the study, the department will be better equipped to determine risk mitigation strategies, the future of legacy systems and processes, and the funding needs of various agencies. This project aims to centralize the disparate solutions currently in use by state agencies.

Technical Questions

Q: Will the new HRIS SaaS be able to eliminate all or most of the listed systems and software?

A: Once the study is complete, a better determination of which systems could be eliminated can be made. It is the Department's intent to create efficiencies and eliminate redundancy.

Q: How were the preliminary estimates for the implementation of the new HRIS system calculated?

A: The preliminary estimate for the new HRIS system was derived from existing research and analysis. The total projected budget is a preliminary estimate, pending an updated comprehensive study, which is the purpose of the Department's FY 2025-26 IT capital request. This preliminary estimate is supported by prior analysis and research that the State conducted to explore the implementation of a statewide HRIS and determine the optimal scope, feasibility, and implementation strategies.

This research, which informed the estimate, includes:

- The 2014 HRIS Budget Assessment developed by Rebound Solutions.
- The 2021 ERP, Payroll, HRIS roadmap developed by Gartner.
- The 2022 Capability Mapping exercise with agencies facilitated by Gartner.
- Extensive interviews conducted by DPA with agency HR and payroll teams between 2021 and 2024.

Q: How will the system handle data security, privacy, and access controls especially for a larger user database?

A: The system has not been selected. Vendor solutions will be evaluated to ensure the system will comply with the State's requirements for data security, privacy and access control.

Q: What is the vendor's implementation methodology for a large enterprise?

A: The vendor has not been selected. Vendors will be evaluated on their proven ability to implement enterprise solutions in a government setting of comparable size and complexity.

Q: Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: The system has not been selected. Vendor solutions will be evaluated to ensure the system meets the State's requirements for data storage, and that the vendor has sufficient redundancy for disaster recovery.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Vendor solutions will be evaluated on the ability to integrate with other State technologies and data sources.

Q: Will the system enable logging and resolution reporting on all issues?

A: Vendor solutions will be evaluated on the ability to provide sufficient logging and resolution reporting to meet the State's requirements.

Q: Will the system provide proactive alerts on system events?

A: Vendor solutions will be evaluated for alerting capabilities from a technology perspective as well as a vendor service level agreement.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role-based access?

A: Yes. The System will support user authentication, password policy management, two-factor authorization, single sign-on and role-based access.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: The Department seeks to avoid customization that would make standard upgrades difficult. The Department prioritizes systems that allow for configurations to meet unique business needs including low-code options so that business users can update user interfaces, tables, process components such as workflow, and business logic. Vendor solutions will be evaluated on this basis.

Q: Will the vendor provide technical support e.g. 24/7 support?

A: We intend that the vendor provide technical support e.g. 24/7 support - vendor service level agreements and support will be part of the evaluation process.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: The Department will evaluate vendor capabilities for training. In other projects the Department has led and/or augmented vendor training so as to deliver tailored training to State users.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, this is part of the Department's standard vendor evaluation process.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes, providing a minimum of two high quality references with organizations in similar government settings is part of the Department's standard vendor evaluation process.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Public Health and Environment

Stationary Sources Technology Modernization

Project Summary

The Department of Public Health and Environment (CDPHE) is requesting state funds for the Stationary Sources Technology Modernization project.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$6,099,148	$1,748,863	$0	$0	$7,848,011
CF	$4,530,695	$0	$0	$0	$4,530,695
Total	**$10,629,843**	**$1,748,863**	**$0**	**$0**	**$12,378,706**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	3 of 8	Recommended for funding.

Project Status

This request is for phase four of a four-phase continuation project. Prior appropriations total about $10.6 million, with about $6.1 million from state funds and $4.5 million from CDPHE's Stationary Source Control Fund.

Project Information

Project Objective

This project replaces data systems used for the department's Air Pollution Control Division (APCD). The outdated database is the primary tool used by the APCD that manages permitting, inspections, enforcement, compliance, billing, emissions, and data reporting necessary for regulating stationary sources.

The current systems date from 1995 and still rely in part on paper-based processes. Additionally, the greenhouse gas reporting system (eGGRT), a subsystem used by the department, is provided by the federal Environmental Protection Agency and is likely to be eliminated. The new system will increase the department's regulatory effectiveness and make processes less burdensome for all stakeholders.

Project Description

Overall, this project is an effort to modernize the systems the department uses for regulatory duties. The new, web-based system will perform a number of functions, such as: application and payment for required permit; uploading documents required by regulations or law; and the ability for each user to update and modify information on file with the Stationary Sources Program (SSP).

Previous phases resulted in implementation of portions of the project. Phase four will continue these efforts, as well as develop and implement a data management system for internal processes and allow for public access. The project uses current technology solutions, primarily Salesforce and Amazon Warehouse Services, to replace existing data systems. The focus of this phase is on the replacement of the eGGRT system and stationary source emissions regulatory processes, but various processes will also receive a digital solution.

All of the funding requested for phase four is for Operating & Professional services, with a nominal amount as project contingency. About $1.3 million is for consultants and contractors, with $300,000 for other operating and professional services costs. The department delayed the request timeline for this project by one year to balance the use of outside contractors with internal staff resources of the Office of Information Technology (OIT). This also allowed the department to evaluate the implementation of phases one and two before beginning phase three.

CDPHE reports that there are few alternatives to this project given the department's duties. Any alternative would result in the continued use of outdated systems and inefficient processes. If

funding is not approved, the department would continue to use its current systems resulting in unnecessarily burdensome processes for the department, external stakeholders, and the public.

Project Planning

The department mentions that OIT is engaged in the procurement and planning process for the project and that the new system will be compliant with OIT's regulations. The department has used a balance of OIT resources and contracted vendors to work on the project. Additionally, the department conducted market research for the eGGRT replacement by contacting the EPA, the vendor for the EPA's current system, and discussions with other states.

In particular, project planning included an analysis of the department's needs, available solutions, and a focus on ensuring the new system has future-proof features. The design of the system with a platform-as-a-service model minimizes the need for an end-of-life determination and can avoid a total system replacement in the future. The department reports that for accounting purposes, the system should have a 30-year depreciation schedule. The decommissioning costs for the current system are minimal, with fewer than 10 hours of services from OIT necessary.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$8,085,553	$1,665,584	$0	$0	$9,751,137
Software	$607,984	$0	$0	$0	$607,984
Contingency	$187,443	$83,279	$0	$0	$270,722
Total	**$8,880,890**	**$1,748,863**	**$0**	**$0**	**$10,629,843**

Cost Benefit Analysis

The department reports that the primary benefit of the new system will be a dramatic reduction in the staff time required for processes. The total savings is estimated at about 24,000 in processing days, and about 2,800 processing hours annually.

Cash Funds

This project received a previous appropriation of about $4.5 million from the department's Stationary Source Control Cash Fund.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Title V Operating Permits	January 2025	June 2026
Remaining Core Processes	July 2025	June 2028
Indoor Air—Asbestos/Lead	July 2026	June 2027
Oil and Gas Reporting	July 2025	June 2027
Planned System Enhancements	January 2026	June 2028
Air Emissions Reporting	January 2026	June 2027
eGGRT Reporting System Replacement	July 2026	June 2028

Staff Questions and Comments

Project Questions

Q: The Available Funds Continuation History indicates about $1.6 million in FY 2023-24 funds are still available. Can you provide information on the plan for these funds?

A: Additional technology projects will be underway later in FY 2025-26 and will use the $1.6 million of funding remaining from the FY 2023-24 IT capital appropriation. These projects include compliance and inspection technology systems, greenhouse gas reporting system enhancements, and replacement of the oil and gas emissions reporting system.

Q: Are there plans for engaging with external stakeholders regarding implementation, such as regulated entities?

A: The department has prioritized stakeholder engagement throughout the life of the project. Before project construction began, the department first surveyed regulated entities for input, and has continued to engage regulated entities since then. The department uses mailing lists to maintain contact with stakeholders. The new system also prompts users to provide feedback about their experience. Lastly, stakeholders can use the department's dedicated project email

address to share their specific user needs. In response to this feedback, the department created additional guidance documents and instructional videos to improve the user experience.

Technical Questions

Q: Will the new eGGRT system be fully integrated with the new data management system?

A: In light of unexpected decommissioning of the federal eGGRT system, the department's immediate intent is to pursue an expedited and more cost-effective method to capture reporting elements. The department could also utilize a re-hosted version of the tool in the future. The goal is for the system to capture data for queries from the common data warehouse and visualization tools.

Q: What was the procurement process that led to the choice of SalesForce and Amazon Warehouse Services being the chosen vendors? Were there competitive bids on this phase of the project?

A: Salesforce and Amazon Web Services are approved by the OIT and supported platforms, used throughout the state. These platforms provide high quality and security, and have proven scalability necessary to meet future demands and avoid technology obsolescence. Their functionality can be adapted for diverse uses, and they are capable of continuous maintenance and modernization. The platforms were chosen to carry our technology stack forward and to avoid end-of-life determination. The department used the OIT's standards, including the State Pricing Agreement, for procurement. Vendors submitted competitive bids and were selected based on price, quality, depth, and experience.

Q: Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: The system provides ample storage capacity for both structured and unstructured data and file types, supports disaster recovery through redundant servers and other tools, and can revert or restore data as needed. These functions are included in the OIT's criteria for approving a platform. Specifically, if a platform cannot meet the OIT standards for security and disaster recovery, that platform will not be approved and supported by OIT.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: The system will integrate with relevant applications and technologies, including Salesforce, Amazon, Tableau, Onbase, and other relevant sources and technologies as needed.

Q: Will the system enable logging and resolution reporting on all issues?

A: The system can enable logging and resolution reporting on issues, and the department is currently working to implement this functionality. Users also have several ways to contact department support staff in order to report issues. For example, an automated correspondence from the system gives the user a chance to share feedback. Users can also directly email department staff dedicated to the Salesforce system to log issues and receive a resolution.

Q: Will the system provide proactive alerts on system events (cybersecurity)?

A: The system has alert notifications that indicate to the department when service disruptions, performance degradation, and maintenance activities occur. Additionally, the system monitors for anomalies and suspicious activities, triggering security alerts when detected.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: The system currently supports user authentication, password policy, two-factor authentication, and role-based access.

Q: Will the system allow customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic?

A: The system uses custom components such as user interfaces, work flows, and rules. Customization is performed in a low, no code manner, allowing for easier maintenance and changes as needed.

Q: Will the vendor provide technical support e.g. 24/7 global support?

A: The vendor provides 24/7 support.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Training is provided by the vendor using online and offline mediums. This was part of the department's request during the vendor bidding process. For tools not created by a vendor, the project team is developing online and offline training for both internal and external users.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Department of Public Safety

Records Utilization Upgrade

Project Summary

The Department of Public Safety (CDPS) is requesting cash fund spending authority for continuation funding of its Records Utilization Upgrade (RUU) project. This funding will support phase three of the project, which includes the Federated Records Advancement and Unified Intelligence Analysis components.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$2,160,581	$0	$0	$0	$2,160,581
CF	$0	$2,564,100	$0	$0	$2,564,100
Total	**$2,160,581**	**$2,564,100**	**$0**	**$0**	**$4,724,681**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	1 of 3	Recommended for funding.

Project Status

This request is for phase three of a three-phase continuation project. Phase one received $525,000 in state funds for FY 2024-25, and phase two received $1.6 million from state funds for FY 2025-26.

Project Information

Project Objective

This project is replacing several independent record management systems used by the department with a new, integrated system. The goal of the project is reducing the time, complexity, and uncertainty associated with current manual, paper-based traffic citation processes. The department currently must access independent systems for record keeping, which increases workload and associated costs. The new system will allow the department to reallocate resources toward direct service to the public.

CDPS states the project includes implementing a Federated Systems Integration (FSI), a two-way exchange between software-as-a-service (SaaS) and platform-as-a-service (PaaS) products and a mobile-centric records systems used by internal and external agency teams. CDPS believes that this approach will improve integration and interoperability of internal and external criminal justice data systems and offer improved analytics, investigatory data services, and strategic reporting. The department notes that the project may improve officer roadside safety due to decreased time spent in high-risk environments.

Project Description

The project started with phase one, a records utilization blueprint and roadmap. Phase two is being implemented and focuses on eCitation capability. Phase three contains two components, Federated Records Advancement and Unified Intelligence Analysis. This last phase is focused on replacing the various record management systems of the department with a single system.

Phase one is complete and has not affected the functionality of current systems. Phase two is underway and upon completion will allow for deployment of an eCitation system. After phase three is completed, the department will have a functional, unified records management system. Agile project planning will apply in phase three on a small scale once application and technology integration occurs. If funding is not appropriated for phase three, the contingency plan is that the department will continue to use existing records management systems.

Project Planning

After phase one, the department used request for proposal (RFP) solicitations for phases two and three. The department also partnered with the Statewide Internet Portal Authority (SIPA) for phases one and three to identify qualified consultants through SIPA's Master Services Agreement (MSA).

The Colorado State Patrol's (CSP) Office of Project Management within the department will coordinate the change management process. This office will support a steering committee composed of the department, partner agencies, and other stakeholders that will also participate in change management. OIT will participate in this process. The project includes relevant user experience testing and training. The costs to decommission the old systems are included as part of the migration to a new platform. Additionally, partner agencies may have costs to modify existing systems, but these partner agencies have submitted letters of support for the project.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$992,339	$315,060	$0	$0	$1,307,399
Software	$467,309	$2,126,940	$0	$0	$2,594,249
Equipment	$623,078	$0	$0	$0	$623,078
Contingency	$77,855	$122,100	$0	$0	$199,955
Total	**$2,160,581**	**$2,564,100**	**$0**	**$0**	**$4,724,681**

Cost Benefit Analysis

The department reports that maintaining the current records management system costs about $3.5 million annually between staff costs and legacy system operations and maintenance. The annual cost of implementing the new system would be about $1.7 million, resulting in a net yearly benefit of about $1.8 million, excluding investment costs.

The lifecycle of the system is expected to be about 10 years based on trends in replacement cycles for public safety technology. However, the use of a software-as-a-service (SaaS) model for this system reduces the obsolescence of both hardware and software.

Cash Funds

The request for phase three of the project is funding from the HUTF. The HUTF is the primary source of state highway funding and receives revenue from motor fuel taxes, registration fees, and other related fees. CDPS receives revenue from the HUTF before other distributions are made and is requesting spending authority from this apportioned revenue.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Phase one—Records Utilization Blueprint and Roadmap	July 2024	June 2025
Phase two—eCitation Functional Capability	July 2025	June 2026
Phase three—Federated Records Advancement, Replace RMS	July 2026	June 2027
Phase three—Unified Intelligence Analysis, Fusion, and Reporting	July 2027	June 2028

Staff Questions and Comments

Technical Questions

Q: Are there standardized mobile printers being recommended? How often do they need to be replaced, and is there consideration for maintenance and replacement of all mobile peripherals and supplies i.e. thermal paper for them in future operational budgets?

A: Yes, standardized mobile thermal printers and peripherals are included in the budget and implementation plan for the Phase 2 electronic citation (eCitation) effort. Small form thermal printers are installed in the Trooper patrol vehicles to print a common standard 4-inch wide durable “slick” ticket. Research indicates a typical printer replacement cycle of 3 to 7 years, based on volume of use. The CSP has estimated future consumables costs for thermal paper as an operations cost. The estimate is based on the average number of current citations issued and market based pricing for thermal paper for this volume of citations.

Q: Will the data that will be collected from the new e-ticketing system be entered into a new data interchange and available to all stakeholders of that data?

A: Yes, eCitation ticket data will be transmitted from the CSP in Javascript Object Notation (JSON) format to the CICJIS. This remains consistent in operation to the proof of concept eCitation project conducted with CICJIS and Colorado partner agencies in 2024 to 2025.

Q: How was the public safety records management consultant selected, were they recommended by anyone or a related organization?

A: The public safety records management consultant (PRI Management Group) was highly recommended by multiple Colorado policing departments, and policing agencies in other states, that had retained records management advisory services from this consultant. As well, the consultant was highly recommended by contacts through the International Association of Chiefs of Police (IACP) and the Integrated Justice Information System (IJIS) Institute. This consultant was selected from proposals received through the State of Colorado documented quote (DQ) procurement process.

Q: Will SIPA be recommending a choice vendors for the Federated Records Management System that offers an eCitation system?

A: Primary recommendations and assistance from the public safety records management consultant formed the basis for comprehensive eCitation functional requirements and specifications included in a competitive through a request for proposal (RFP). The eCitation and RMS requirements and specifications have been jointly analyzed and developed with specific emphasis on open data standards and data integration and system interoperability features.

Q: Will the system provide proactive alerts on system events i.e. cybersecurity feature?

A: Yes. All system components of the RUU (Phases 2 to 4) require functional and non-functional requirements specifications to provide continuous proactive monitoring and alerting for internal, external system events. These alert features are consistent with the current recommendations by Colorado Office of Information Technology (OIT) to leverage contemporary system security features for Identity and Access Management (IAM), System for Cross-domain Identity Management (SCIM), system operations stability and performance (Telemetry) and other real time alerting service capabilities.

Q: Will this system integrate with all relevant applications, data sources and technologies used at CSP?

A: Yes. A core principle developed in the Phase 1 enterprise architecture, blueprint and roadmap, is mandatory systems integration, interoperability and data exchange. This integration focus is embedded for all specifications of RUU system components, guided by system selection and system implementation guidance developed in the Phase 1 enterprise architecture reference guidance. An analysis of the most significant current CSP legacy systems that will remain in

operation alongside the RUU systems are expected to be fully interoperable. This is due to the common integration capabilities (e.g., Application Programming Interfaces {APIs}) already available in these significant legacy systems.

Q: Data Storage- Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: Yes. The significant benefit of the systems architecture specification for all RUU system components involves contemporary secure cloud hosting environments. These modern cloud platform and SaaS solutions provide very large and highly available data environments that "scale on demand" and leverage economies of hyperscale data centers, with robust continuity of operation and disaster recovery failover capabilities. Moreover, all hosting and individual SaaS solutions (e.g., eCitation and RMS) provide contractually defined, precise, historical data snapshots and archives serving rollback capabilities, and management of data in compliance with records retention schedules.

Q: Will the system enable logging and resolution reporting on all issues?

A: Yes. Referencing the response to Technical Question #5, all RUU solution components include service level requirements for contemporary telemetry information in alerting and operations logging. This includes system monitoring information in a) operation metrics, (aggregated numerical data over time, for request rates, error counts, and system utilization), b) logs (timestamped events that have occurred within the systems) and, c) traces: (system activity and data stream, path and timing of requests through different components across systems)

Q: Will the system support user authentication, password policy management, two-factor authorization, single sign-on and role based access?

A: Yes. The Phase 1 enterprise architecture reference guidance provides universal technical requirements to guide specification and selection of RUU system solutions. The requirements include Security Requirements, Identity and Access Management (IAM) Requirements, Integration and Data Portability Requirements, and Infrastructure and Governance Requirements.

Specific requirements for IAM, include solution provider capability to support Strong Authentication with MFA (multi-factor authentication) and integration with enterprise identity providers (SAML, OAuth, OpenID Connect); Role-Based Access Control (RBAC) assigned permissions based on least privilege principles; and, Audit Logging of authentication, authorization, and access events.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings, i.e. State Patrol Department, Public Safety Department

A: Yes. CSP is working with the Colorado Department of Public Safety (CDPS) Office of Procurement to ensure that RUU solution procurement RFPs include at least three verifiable references of where solution providers have currently implemented services and products with public safety and policing agencies.

Q: Will there be a Service Level Agreement (SLA) with the vendor?

A: Yes. Contractual SLA terms are critical for SaaS and cloud hosting solution services. All solution provider contracts will include quantified and monitored SLAs. The SLAs will be specified in a Vendor Master Services and Purchasing Agreement (MSPA), as well as necessary addendums to the MPSA completed in the contract negotiation process to complete a final solution contract.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Yes. The CSP includes contemporary training, advanced learning, user assistance and change management are specific requirements in the solution procurement RFP. These requirements are specific to initial implementation and ongoing operations (e.g., of high importance in operations, for future solution software feature upgrades and changes)

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Pueblo Community College

Wireless Network Upgrade

Project Summary

Pueblo Community College is requesting $824,373 in state funds for wireless network infrastructure upgrades across multiple campus locations.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$824,373	$0	$0	$824,373
CF	$0	$0	$0	$0	$0
Total	**$0**	**$824,373**	**$0**	**$0**	**$824,373**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Colorado Commission on Higher Education	1 of 10 (tied)	Recommended for funding.

Project Status

This is a new project. PCC requested funds for a project including wireless upgrades in FY 2017-18, which was not appropriated funding. PCC includes no additional IT capital projects on its five-year capital plan.

Project Information

Project Objective

PCC is requesting funding for a full replacement of its wireless Access Points (APs), cabling and other associated resources. PCC states that existing wireless network infrastructure is becoming obsolete and cannot accommodate increasing demand on the system. PCC states that increased use of artificial intelligence applications is increasing demands on network bandwidth.

In addition to increased capacity from the upgrade, the college indicates that there are unsupported APs that no longer receive security updates, and that others are near this phase as well. This creates a cybersecurity risk for both the college and possibly the Colorado Community College System (CCCS) due to a shared network. When asked by staff specifically about CCCS confirming the risk to their network, PCC confirmed that, "the existing infrastructure can function securely within the CCCS shared network for several more years" and that not receiving funding would not pose an immediate security risk.

PCC reports that physical safety is relevant to the project as well in allowing public safety officers the ability to communicate and effectively lock doors in real time during an emergency. The college states that the network supports the PCC public warning system and the ability for public safety officers to observe surveillance cameras while in their vehicles. Finally, the project will also allow for more reliable WiFi-calling, which is necessary on the college's Mancos and Cañon City campuses, which have unreliable cellular service.

Project Description

PCC states that the project will provide upgrades to Pueblo, Mancos, Durango and Cañon City campuses. According to PCC, the request includes replacement of the following:

- approximately 450 Wireless Access Points;
- approximately 20 Meraki/Cisco Access Point switches; and
- network cabling, replacement cables and connections.

PCC has upgraded core switches and wireless controllers and will upgrade APs with this project. The college describes how the request is in line with the Colorado Department of Higher Education Strategic Plan by improving the college experience for students in urban and rural parts of the state. The college emphasizes the importance of reliable wireless access for faculty and students in order to provide a high-quality education experience.

Project Planning

The college states that its IT Services unit performed an analysis of the current environment and consulted with several external independent vendors to inform the request amount. The college intends to begin the project with a final consultant-supported design review, which staff confirmed is accounted for in the professional services line item of the request, and encompasses consulting and contractor costs for the project. In addition, PCC states that the college IT Services department, as well as CCCS IT, has dedicated technical staff who will provide oversight of the project. While PCC plans to perform much of the labor and implementation in-house, the college also plans to make use of the prospective vendor's support team to the fullest extent possible.

PCC states that operating costs associated with the project will be covered by PCC and the IT Services budget or through other funding outside of the IT capital process. The college does not plan to make additional requests associated with the project. PCC indicates that standard networking best practices places an expected lifespan of APs and switches of five to seven years.

The college states that it has used quotes from current vendors for an understanding of expected hardware costs. When asked by staff about whether research will be conducted on vendor financial health, the college states that equipment will be purchased from Cisco for both switches and access points and that Cisco is a standard vendor for CCCS.

Cost Information

Table 3
Updated Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$63,846	$0	$0	$63,846
Software	$0	$169,344	$0	$0	$169,344

Equipment	$0	$591,183	$0	$0	$591,183
Total	**$0**	**$824,373**	**$0**	**$0**	**$824,373**

The Cost Summary sheet of PCC's request includes line-item totals that add up to $1,057,563. However, the first page of the request includes a table which aligns with the totals above. In addition, in the prioritization tables submitted by the Colorado Commission on Higher Education (CCHE) and OSPB, as well the college's 5-year capital plan and elsewhere in the request, the $824,373 total is referenced, indicating that the cost summary numbers are inaccurate.

Cost Benefit Analysis

The college was unable to provide a cost-benefit analysis (CBA) as required by Section 24-37-304(1)c.5)(V), C.R.S. However, PCC states that the upgrade will decrease network outages, which will result in savings from eliminating lost work time associated with outages. When asked whether the college can provide a CBA, the college provided the following points:

- an estimated 20 percent reduction in annual maintenance and support costs compared to legacy systems, due to fewer breakdowns and lower support contract costs;
- a reduction in labor associated with addressing an outage, reducing IT costs in parts and labor to resolve issues;
- indirect savings from cancelled classes and instructional work loses caused by an outage which typically lasts 30 minutes to 4 hours; and
- savings from lower energy consumption from new more efficient equipment.

Cash Funds

The request does not include a cash fund component. Of note, CCHE uses scoring criteria for ranking higher education institution projects. The ranking includes an "Other Fund Sources" component, which incentivizes institutions in contributing cash funds in their requests. However, CCHE exempts certain institutions, including PCC, from this criterion.

PCC reports that the college has already contributed approximately $92,000 from campus funding sources for two Cisco CW9800 wireless controller upgrades, as well as two Exagrid backup appliances, which it indicates is complimentary to the larger wireless upgrade. When asked about whether this investment can stand alone from the request, PCC confirmed that it does and that the new wireless controllers were purchased to accommodate the new access points and switches.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	June 2025	July 2025
Design	August 2025	December 2025
Procurement	February 2026	March 2026
Testing	May 2026	June 2026
Outdoor Deployment	June 2026	August 2026
Indoor Deployment	November 2026	August 2027
Remaining Deployment	July 2027	August 2027

Staff Questions and Comments

Technical Questions

Q: Will the network antennas be able to be placed at a safe distance on campus that meet FCC limits for public exposure?

A: The FCC Maximum Permissible Exposure (MPE) limits for RF energy that is considered safe for the public at distances of approximately 8 inches, has been factored into outdoor AP placement. All of the existing outdoor AP antennas being replaced will be installed at the roof level of buildings. This distance should be more than sufficient to satisfy the FCC and device manufacturer requirements for safety and best practices.

Q: How robust is your cellular service from significant cell carriers?

A: With the exception of our Canon City campus, the cellular service at all the PCC campuses is robust. There are cellular towers at each of the campuses. We don't anticipate any more cellular coverage issues at the college than we have currently.

Q: If some cell carriers have weak connections, are you planning on conversing with any of them to boost cell services around campus?

A: PCC has cell towers and services at each of its campuses, with equal coverage between brands such as T-Mobile, Verizon, and AT&T. For campuses where cell coverage is not ideal, such as our Canon City site, IT Services has been in contact with Verizon to explore ways to enhance coverage, possibly with satellite to cell service. With the federal and state prison systems and a

unique geology at the Canon City campus, cell coverage has been a particular problem. Yet, we are excited that this new service could resolve connectivity issues. Yet, even if this becomes a future option, PCC will also have to vet the service with CCCS-IT to ensure that security is maintained and that it remains cost-effective.

Q: Does the campus have a redundant internet provider for emergencies?

A: CCCS System Office provides network service to all PCC campuses through the CCCS Wide Area Network (WAN). CCCS-IT has redundant internet routes and plans in place to offset potential outages.

Q: Have the number of users and devices been calculated to match wireless bandwidth required?

A: Because the newer standard frequencies have changed distance requirements, a site survey will need to be conducted through consultation services or in-house to ensure that the newer standards for WiFi 6e and 7 have been met. We don't anticipate this survey requiring an off-site evaluation, since our own networking team does have the tools and knowledge to complete the survey. Yet we are also open to an outside consultation as well.

Q: Will security measures be implemented that include encryption protocols (WPA3) authentication methods such as 802.1X and network segmentation?

A: Security measures such as WPA3 will be implemented with the new wireless upgrade and comply with those of CCCS, as well as networking best practices (currently WPA2/WPA3 mixed mode). The wireless controller in place is capable of WPA3. As access points are upgraded, WPA3 will be in full implementation. PCC will always ensure that security is a top priority for campus, faculty, staff, and student data. Network segmentation with VLANs and subnetting is already in place.

Q: Will there be different levels of network access for different users e.g. separate networks for staff, students, faculty and guests?

A: PCC already has a separation of WiFi and wired networks in place. There is an Instructional network that is dedicated to Faculty, an Administrative network separate for staff and administration, and there is an open PCC Guest network for students and visitors.

Q: How will access to the network be authenticated? Will it use existing campus credentials or a different system?

A: PCC is open to developing a different process for authentication, as standards and best practices call for changes. But for the initial upgrade, PCC will use its current authentication process based on our local Active Directory. For students, with multiple devices and brands of

computers, we have a guest network with terms and conditions that must be accepted for connection.

Q: Will the system provide proactive alerts on system events?

A: PCC already has several proactive system alerts in place with Public Safety, including AppArmor and Linx 911/MyPCC Alert software. Every Instructional and Administrative computer at the college has proactive alerts in one or both services.

Q: Will the vendor provide technical support e.g. 24/7?

A: The vendor will provide technical support for issues that cannot be resolved in-house by the PCC networking team. This is part of a service plan that is purchased with the switches and access points, and is a best practice when implementing new networking equipment. The vendor will provide 24/7 support.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Equipment will be purchased from Cisco for both switches and access points. Cisco is a standard vendor for the CCCS. Cisco is a major brand in the networking industry and reported a 5% year-over-year revenue increase for FY2025, reaching $56.7 billion, with Q4 2025 revenue up 8% year-over-year to $14.7 billion. They will continue to be a leader going forward and we don't anticipate any issues in using them.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Cisco is in use at a majority of all CCCS colleges. We are very confident that we can get multiple references from the vendor for serviced colleges in the CCCS system.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

University of Northern Colorado

Life Safety Technology Modernization

Project Summary

The University of Northern Colorado (UNC) is requesting a combination of state funds and cash fund spending authority to update and standardize critical life safety systems.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$1,861,248	$0	$0	$1,861,248
CF	$0	$120,912	$0	$0	$120,912
Total	**$0**	**$1,982,160**	**$0**	**$0**	**$1,982,160**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	7 of 8	Recommended for funding.
Colorado Commission on Higher Education	1 of 10 (tied)	Recommended for funding.

Project Status

This a new, never-before-requested project. UNC is requesting $1.8 million in state funding and $120,000 in cash fund spending authority for a single-phase project.

In FY 2024-25, UNC was appropriated $5.3 million in state and cash funding for the Wireless First project to transition from wired internet and physical phone connectivity to a wireless network in every academic, residential, and administrative area of campus. In FY 2023-24 UNC was appropriated $1.3 million in state and cash funding for the ERP Modernization and Cloud Transition to move the institution's on-premises ERP system to Ellucian's Managed Cloud.

Project Information

Project Objective

The goal of this project is to replace obsolete computer hardware, modernize communication systems, decommission analog phone lines, implement hardware and software that hosts the fire protection system to ensure resilience, enhance cybersecurity, and address accessibility standards in an effort to upgrade and standardize UNC's critical life safety systems.

If this project is not funded, UNC states the following consequences:

- noncompliance with state and federal accessibility laws;
- increased likelihood of critical failures during emergencies;
- increased vulnerability to outages and disruptions without backup; and
- increased vulnerability to cyber threats.

Project Description

UNC first plans to address is security threats. This project would fund upgrading to Windows 11 compliant devices, thus providing more resilient cybersecurity. Additionally, it will update the fire alarm system and ensure access to critical security upgrades. This will include the ability for cellular backup to ensure life safety systems will be operational even in the event of a network disruption or cyber incident.

The project will consist of updating and replacing several software and hardware technologies. This entails replacing analog elevator emergency phones, upgrading the elevator communication system, and upgrading elevator controls.

Project Planning

The UNC Project Management Office will be assigning a project manager that will review and update the initial scope of the project. UNC has a defined maintenance window that will not be disruptive to students. Stakeholders and technical staff will work together to establish

procedures and policies, including a communication plan to keep students, teachers, and staff informed.

Additionally, UNC's Information Management and Technology, Facilities Management, Disability Resource Center, and Rocky Mountain ADA Center will all be involved in the project to ensure the intended goals will be met.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$0	$0	$0	$0
Software	$0	$91,899	$0	$0	$91,899
Equipment	$0	$1,795,872	$0	$0	$1,795,872
Contingency	$0	$95,389	$0	$0	$94,389
Total	**$0**	**$1,982,160**	**$0**	**$0**	**$1,982,160**

Cost Benefit Analysis

UNC stated that if the project is funded, compliance penalties and ongoing maintenance costs would be avoided. It is predicted that the following approximate savings would occur annually:

- $60,000 from removing analog phones;
- $5,000 from removing obsolete servers; and
- $2,400 by removing unsupported operating systems.

Cash Funds

The cash funds for this project come from the institution's operating funds.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Pre-Design	April 2026	October 2026
Design	October 2026	March 2027
Procurement	March 2027	April 2027
Implementation	April 2027	September 2027
Go-Live	September 2027	December 2027

Staff Questions and Comments

Project Questions

Q: UNC was appropriated $5M in FY2024-25 for the Wireless First project. How does this project differ and how will they work together?

A: This project is the final step in one of the Wireless First objectives. As part of the Wireless First project, UNC is reducing the number of physical ports on our network. With a new robust Wi-Fi, UNC will pivot to Microsoft Teams Voice instead of physical phones. Once we remove physical phones, the only remaining "legacy" voice infrastructure is our elevator and life-safety equipment. This project is the last step to completely remove our Cisco Voice infrastructure, resulting in a significant reduction in software costs and eliminating the responsibility/overhead of supporting two voice infrastructures.

Q: What is the projected life expectancy of this system? Is there a cost to decommission the old system?

A: There is no cost to decommission the old system. The project's life expectancy is difficult to quantify, but our estimate is a minimum of 10 years.

Technical Questions

Q: How was the Horizon platform chosen above Honeywell and Onyx, was a consultant used to assist in the decision?

A: UNC consulted with multiple vendors to propose a solution that is compatible with our existing systems. ONYXWorks was not considered as it has been discontinued. Horizon is the Honeywell/Notifier product intended to replace the discontinued ONYXWorks System. Horizon is most likely to be selected because it is compatible with our existing mix of Honeywell and Notifier Systems.

Q: What is the backup plan for power outages if the cellular access points lose power during an internet outage e.g. loss of power over Ethernet?

A: Emergency/Back-up power will be provided, as required by code, for all systems.

Q: What will be the monitoring capabilities and protocols for dispatching emergency services?

A: The UNC Police Department currently monitors the fire alarm panels and the elevator emergency phones. No changes will be made to protocols for dispatching emergency services. Use of an outside vendor to monitor the elevator system may be considered as the project is implemented.

Q: Will the new emergency systems allow remote monitoring?

A: Yes, both systems are required by code to communicate with remote 24/7 monitoring locations

Q: Can the Audio and Visual alarms be integrated with the campus emergency notification system?

A: Fire Alarm – Many of our existing Fire Alarm systems do not use modern voice-based notification systems and, as such, are unsuitable for use beyond communicating Fire Alarm conditions. UNC has previously consulted with our AHJ, the Greeley Fire Department (GFD), to request permission to integrate non-fire alarm emergency notification with existing fire alarm systems that utilize voice-based notification. To date, GFD has been reluctant to allow this integration. UNC will request and evaluate this integration capability as we procure a vendor. UNC will continue discussions with GFD to seek permission to integrate these systems.

Elevator – Yes, our goal is to have both Audio and Visual alarms be integrated.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Yes, this project addresses integration with all applicable technologies and data sources.

Q: Will the system enable logging and resolution reporting on all issues?

A: UNC has robust logging and mature problem resolution procedures.

Fire Alarm – Yes, this is a standard automatic function of this system. Elevator – Yes, event logging occurs automatically.

Q: Will the system provide proactive alerts on system events?

Fire Alarm – Yes, this is a standard automatic function of this system.

Elevator – Yes, this capability will be required as we procure a vendor to provide the solution.

Q: Will the System support user authentication, password policy management, two-factor authorization, single sign-on, and role-based access?

A: Yes, these systems will be part of our enterprise account management policies. Those policies include modern security requirements, such as strong password policies (complexity and expiration), multi-factor authentication, and access to the HVAC-specific VPN realm. Additionally, we adhere to the principle of least privilege with role-based access to all enterprise systems.

Q: Will the vendor provide technical support e.g. 24/7 global support?

A: Yes, these capabilities will be required as we procure a vendor to provide the solution.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: Yes, these capabilities will be required as we procure a vendor to provide the solution.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes, we have been researching best-in-class vendors, and we will require financial disclosure as part of our procurement process.

Q: Will the vendor provide a minimum of two high-quality references with organizations in similar government settings?

A: Yes, we will require up to three references as part of the procurement process.

Joint Technology Committee

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Fiscal Year 2026-27 IT Capital Budget Request

Western Colorado University

Digital ID, Security & Access

Project Summary

Western Colorado University (WCU) is requesting state funds for a new Digital ID, Security & Access project.

Table 1
Prior Appropriation and Request Information

Fund Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
CCF	$0	$7,812,362	$0	$0	$7,812,362
CF	$0	$78,913	$0	$0	$78,913
Total	**$0**	**$7,891,275**	**$0**	**$0**	**$7,891,275**

Table 2
Project Prioritization

Prioritized By	Priority	Notes
Office of State Planning and Budgeting	0 of 8	Not recommended for funding.
Colorado Commission on Higher Education	7 of 10	Recommended for funding.

Project Status

This is a new, single-phased project with no prior appropriation.

Project Information

Project Objective

The project aims to both replace the current WCU campus security infrastructure and add new functionality. The current campus security infrastructure is largely a patchwork of solutions implemented in the past, many of which are reaching or are at end of life and vendors will no longer be providing support. The project will implement a solution utilizing identification services, physical access control, and additional security enhancements. WCU notes recent high-profile incidents on college campuses across the nation and the presence of valuable equipment on its campus as reasons for an enhanced security infrastructure.

Project Description

WCU indicates that this is a single-phase project. The amount requested will be spent across three primary components:

- digital ID and service access;
- physical access control; and
- additional security enhancements

Digital ID and service access includes implementing a digital identification platform for services on campus. The digital identification will be used to manage dining, door access, log event attendance, facility access, and access other services on campus. Additional security enhancements include replacing existing surveillance cameras and expanding the total amount of cameras on campus from 52 to 250. Most of the requested funding will be spent on physical access control, which involves upgrading and expanding controlled access doors on campus from 427 to 1,757. Expenditures for this component are estimated at about $5.8 million. The total amount requested represents full or maximum deployment of the proposed security solution across campus.

WCU plans to implement the project over about two years, working around the academic calendar to minimize the impact on students. WCU will first deploy digital ID for services, then acquire equipment for the other components. Finally, digital ID will be deployed for controlled access on campus. If funding is not provided, WCU will address failing components first and delay implementing a more comprehensive campus security infrastructure.

Project Planning

WCU reports that it received eight responses to a request for information (RFI) for this project. If the project is funded, they will proceed with a request for quote (RFQ) to secure the best offer from all vendors. The amount requested reflects information provided in the RFIs. JTC Staff highlights that this amount reflects the maximum or full deployment of controlled access for every door on campus. WCU indicates that the projected life expectancy for the door access control component is 10 to 15 years, while the security camera system is expected to last 5 to 10 years.

Most of the staff necessary for the project will be contracted, but WCU will assign a Project Manager and Budget Analyst to monitor the project. WCU will begin with a full-scale pilot of the solution in one campus building to ensure it functions as expected before implementing on all campus buildings.

Cost Information

Table 3
Itemized Cost Information

Cost Source	Prior Appropriation	Budget Year FY 2026-27	Out Year FY 2027-28	Future Requests	Total Costs
Professional Services	$0	$2,894,860	$0	$0	$2,894,860
Software	$0	$1,032,640	$0	$0	$1,032,640
Equipment	$0	$3,276,000	$0	$0	$3,276,000
Contingency	$0	$687,775	$0	$0	$687,775
Total	**$0**	**$7,891,275**	**$0**	**$0**	**$7,891,275**

Cost Benefit Analysis

WCU identified minor direct savings from implementing this project, about $10,800 annually from no longer issuing physical identification cards and keys. Additionally, in the event a current physical key is lost, rekeying the entire campus costs about $220,000. Overall, operational improvements for campus are the primary benefits from implementing the project. Staff would be redirected to more critical functions, and an enhanced security system could mitigate the impact and occurrence of threats on campus.

Cash Funds

Institutional funds are the source of cash funds for this project. Though not included in the estimate for the amount requested, WCU reports it will earmark about $234,000 in additional cash funds for this project, bringing WCU's total contribution to about $312,000.

Project Schedule/Timeline

Table 4
Project Schedule

Project Actions	Start Date	Completion Date
Purchasing, Acquisition and Contracting	May 2026	August 2026
Planning and Design	September 2026	December 2026
Deployment of Digital ID for Services	January 2027	April 2027
Equipment Acquisition	January 2027	April 2027
Installation and Construction	May 2027	December 2027
Deployment of Digital ID for Access Control	January 2028	June 2028
Project Closeout	N/A	June 2028

Staff Questions and Comments

Staff Comments

This request represents WCU's preferred solution for a comprehensive, full-scale campus security system. JTC staff does not question the merits of such a solution. However, JTC staff believes that if the committee were inclined, funding could be approved for less than the full amount requested to reflect a narrower focus on only certain components of the project.

Project Questions

Q: Recently, the JTC has required departments and institutions to provide quarterly progress reports upon receipt of IT capital funds. Will there be any obstacle to providing updates if the project(s) receives funding this year?

A: No.

Q: Is WCU able to use any master agreements for this project?

A: WCU has not yet chosen a specific solution or vendor, but if a master agreement were available for the solution that offered favorable terms, we would certainly take advantage of it.

Q: What are the obstacles to using the existing state digital ID system for WCU?

A: We had not considered using MyColorado, but it would be an interesting possibility to investigate. Challenges might include:

- Approximately 30% of our student population are non-residents;
- Ability of Western to support and troubleshoot MyColorado digital ID's; and
- Technical integrations with chosen security system.

Q: What research was done to follow Statistica's recommendation for 12 percent inflation? Are there any examples of other institutions that have used the same assumption?

A: The market spend on Software as a Service (SaaS) products continues to surge. We felt we needed a separate rate for the part of the project (Software Acquisition) that relied on SaaS. Statista was able to provide an inflation rate for (SaaS) products. Other sources do provide similar rates/trends in spending on SaaS (Vertice). We are not aware if other institutions are using Statista. For Professional Services we used the Bureau of Labor Statistics's Information Technology, Hardware & Services rate of 6%.

Technical Questions

Q: Is there a possible Plan B, that does not include a Digital ID system, it could reduce cost of the project?

A: There is no specific Plan B, but the cost of the project can be scaled by a strategic reduction of the number of doors that would be equipped with electronic hardware. While you would reduce the effectiveness of some features (e.g. campus lockdowns), with thoughtful deployment we could still reach most of the goals of this project.

Q: Is there consideration for the Digital ID System to be implemented as a test system first, as there are some vulnerabilities that are inherent to Digital ID Systems e.g. device compatibility, power outages, malfunctions, or general technical difficulties.

A: Yes, the Digital Credential would be rolled out in phases and assessed.

Q: Is there an alternative solution for those students or faculty/staff that may have privacy concerns who may be uncomfortable with their personal devices being used for campus access?

A: Yes. It is unlikely we would be able to use Digital ID's for in every scenario. Part of the solution would include a small implementation of traditional systems, e.g. ID Cards, FOBs or other

devices that would be used for situations where digital ID is not practical and those individuals that do not have a device or have privacy concerns.

Q: If the Internet Service Provider fails what will be the redundancy and failover mechanisms, including the capacity to run during power failures?

A: Western has two Internet Service Providers using two geographically diverse fiber paths to campus. Internet outages are now very rare. Also, in most cases, the devices on campus (e.g. door controllers, cameras) do not require an active internet connection for routine function, only to make changes. For power outages, our network infrastructure is supported by battery backups that provide power for most minor power outages (one hour or less). This project would augment backup power where needed. Finally, all doors will be equipped with a backup "hard key" option that could be used in the event of a long-term power outage.

Q: Does the vendor hold any certifications related to security and operational excellence e.g. ISO 27001, SOC 2 Type II, etc.?

A: A vendor has not yet been selected. Security certifications such as ISO 27001, NIST and SOC will be required and incorporated into the contracting process.

Q: Will the door access control system integrate with existing security infrastructure including video surveillance and alarm systems?

A: Western currently has only a very small and currently disjointed (multiple vendors) video surveillance and alarm system. This project is expected to replace all the existing infrastructure with an integrated system.

Q: Data Storage- Does this system provide ample storage capacity for data, file types and locations and supports processes such as disaster recovery, rollbacks, extraction or eradication?

A: We have not yet selected a vendor/solution but, yes, part of the solution will be a management system that manages storage, DR and removal of unneeded data.

Q: Will this system integrate with all relevant applications, data sources and technologies?

A: Yes, the proposed system would fully integrate door access control, security cameras, notifications, and digital ID.

Q: Will the system enable logging and resolution reporting on all issues?

A: Yes, the system will do event logging and reporting.

Q: Will the system provide proactive alerts on system events?

A: Yes.

Q: Will the vendor provide technical support e.g. 24/7 support?

A: Yes.

Q: Will the vendor provide best-in-class training and assistance for users using online and offline mediums?

A: The primary support for our users will remain Western staff, but the vendors will be required to provide top quality training and support.

Q: Will some research be done on the vendor health, e.g. is the vendor in a strong financial position?

A: Yes. Only established vendors with multiple clients in a higher education setting are being considered.

Q: Will the vendor provide a minimum of two high quality references with organizations in similar government settings?

A: Yes. Only established vendors with multiple clients in a higher education setting are being considered.