Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@state.co.us • leg.colorado.gov/lcs

Memorandum

January 17, 2022

TO: Joint Technology Committee Members

FROM: Luisa Altmann, Senior Research Analyst, 303-866-3518
Joint Technology Committee Staff

SUBJECT: JTC Staff Analysis of JBC-Referred FY 2022-23 Operating Budget Request
Colorado Department of Public Safety
R-12 Community Corrections Information and Billing System Maintenance Support

Summary of Request

The Colorado Department of Public Safety (DPS) is requesting $425,922 General Fund for FY 2022-23 and $286,602 General Fund for FY 2023-24 and ongoing, with a 3.0 percent annual increase, for contracted hosting, security, and maintenance costs associated with the new Community Corrections Information and Billing (CCIB) system. The Joint Budget Committee (JBC) has asked the Joint Technology Committee (JTC) to provide a technical review of this request.

Request Details

Staff from the DPS Office of Community Corrections, the 22 Community Corrections boards, and each of the 30 residential and nonresidential Community Corrections facilities on Colorado use the CCIB system to track clients who are serviced by the Community Corrections system, what services they receive, and their outcomes. The system is also the exclusive method by which Community Corrections contractors and subcontractors request payments for services provided to Community Corrections clients.

DPS was originally appropriated $2.2 million through the IT Capital budget process for development of the new CCIB system in FY 2019-20. When DPS first received this funding for initial system implementation, the department estimated the annual operating costs would be approximately $222,222. The department expects to launch a minimally viable product on June 30, 2022, with development of the second phase of the project continuing through FY 2022-23.

This request will allow DPS to provide ongoing licenses, support, and hosting for the system. According to DPS, the Governor's Office of Information Technology does not have resources or training to support either the ongoing maintenance or the hosting of the hardware.

The department provided the following cost estimates for this request:

Annual Support and Maintenance Costs

- FY 2022-23: $346,680 (2,568 yearly development hours at an hourly rate of $135)
- FY 2023-24: $207,360 (1,536 yearly development hours at an hourly rate of $135)
- The department anticipates that the yearly development hours will remain constant for future fiscal years while the hourly development rate will increase by 3 percent each year.

Annual Hosting Costs: $44,226.12

- Proxy server to internet: $272.61 per month
- Application server: $449.04 per month
- SQL database server: $1,607.24 per month
- Domain controller: $321.68 per month
- Veeam backup server: $272.61 per month
- Watchguard SEIM appliance: $259.30 per month
- Qualys scanning appliance: $213.00 per month
- Firewall and internet: $290.03 per month

Annual Security Costs: $35,016

- OS/Device vulnerability scanning with compliance reports; web application scanning: $1,317 per month
- Tripwire integrity monitoring on files, database schema, AD changes, and firewall configuration: $328 per month
- MDR with 24x7x365 Security Operations Center covering all devices and internet egress points: $868 per month
- Remediation efforts for non-IT and non-development findings: $405 per month

Options for Committee Action

The JTC has three options for committee action when it provides a technical review of an operating budget request to the JBC. The JTC can:

- recommend the request to the JBC for funding with no concerns;
- recommend the request to the JBC for funding with concerns; or
- not recommend the request for funding with concerns.

Question Responses Provided by the Department

1. **Please provide an update on the new CCIB system development. The spending authority for the original IT Capital appropriation for the project from FY 2019-20 expires on June 30, 2022. Please provide an update regarding how much of the original $2.2 million appropriation for the project has been spent and encumbered to date and what the total final project cost is expected to be. Is the department expecting a successful launch of the new system by June 30, 2022?**

   Development is on track and we are expecting a successful launch of the minimally viable product (MVP) on June 30, 2022. To date we have spent $1,187,145.97 out of the total of $1,710,080.00 encumbered. The original scope of the project included a Phase 2 with additional functionality beyond MVP. However, while Phase 2 was part of the original scope, completing it will cost more than was initially estimated by the vendor and will require the use of previously set aside contingency funds. In Quarter 3 of FY 2021-22, the Department will encumber the remaining $479,360.75 to continue development of Phase 2 through FY2022-23.

2. **The original request for the new CCIB system from FY 2019-20 indicated that the estimated ongoing operating expenses for the new system were expected to be $222,222. Please explain why the amount now being requested in ongoing maintenance operations is higher than originally estimated.**

   The original estimate of $222,222 annually was derived from a Request for Information (RFI) conducted for this project in FY 2018-19, which could not account for changes to the actual costs of systems and services in future years. While it was a best effort at estimating future costs for an unknown system, further examination of the system needs as well as better realized system requirements and vision after iterations of the Agile process resulted in a more accurate depiction of ongoing costs. The original request did not take into account the initial cost to maintain and support the system once it is deployed to the customer base, as well as continuous system improvement and updates. Once a system has been released, the first year of maintenance is estimated to be higher as issues not caught during testing are found due to having a more variable user base and user environments.

   Also, due to the Agile development structure of this project, discovery of new features that will both improve the user experience and the value of the system have been found as development has progressed.

3. **What work is the department engaging in now to try to limit the number of bugs and additional functionality that may be needed after the system is launched?**

   The CCIB 2.0 project adheres to the principles of the Agile framework. This means that functionality is being built in increments (sprints), and tested repeatedly throughout the process. On the development end, this means a minimum of 80% test coverage of all code in accordance with the contract. Additionally, to ensure the proper functionality of the User Interface (UI), during each sprint the team has involved an expanded group of Office of Community Corrections

(OCC) testers as well as attaining the assistance of the OIT Business Analyst and IT Project Manager. As the system is built and designed through the Agile process, extensible administrative functionality has been added. This functionality allows the OCC system administrators greater ability to customize the solution and correct issues without the development intervention than the current CCIB 1.0 system.

Currently, the project team is creating a User Acceptance Testing (UAT) environment with data that is reflective of production data to ensure the UAT is as accurate as possible. The OIT Business Analyst will complete a detailed regression testing plan in this environment. Once that is complete, the project will engage end users from a variety of roles (Providers, Judicial Districts, Programs, OCC) to conduct an extensive, coordinated user acceptance testing prior to the "go live" date. Finally, OIT has completed both an architecture and security review of the system.

4. **The budget request explains that OIT "*currently does not have the resources or training to support DPS with either the ongoing maintenance for the hosting of the hardware*." Please provide more details, from a technical perspective, regarding the OIT options the department considered leveraging and why the OIT support was determined to not be sufficient.**

The decision to use the vendor to support the system goes hand in hand with the decision to have the vendor provide ongoing support for the solution. In terms of costs, the vendor's hosting price (which included server and database licenses) was far less than estimates from OIT. In terms of OIT's capability to meet the solution's hosting needs, OIT has very few FBI Criminal Justice Information Security (CJIS) cleared technical support personnel for both maintenance of the solution hardware and coding development. In terms of the solutions environment, OIT lacks a completely redundant, CJIS compliant hosting option that would meet solution business continuity and disaster recovery needs.

Since the CCIB 2.0 solution is hosted by and will continue to be developed by the vendor (Mainstream Technologies LLC), logistics of OIT providing hardware, server, and development support would be extremely challenging. OIT personnel would not only have to learn the solution code, they would have to integrate with the vendor's coding design and architecture. Integration of the continuing development, deployment, and release practices between vendor and OIT would also be necessary to maintain the solution versioning integrity, which would cause further complication and risk to the solution's integrity. Given that the vendor is already familiar with the solution code, the solution functionality, and the underlying solution architecture, there is less complication and risk in having them provide solution support.

Ultimately however, the state of Colorado still owns the code and data for this solution. If at any time a transition away from the current vendor is deemed necessary, the Department has the ability to procure another vendor, OIT or outside of the state, to support the solution.

5. **The budget request explains that "*ongoing maintenance will ensure that the system has the required security to protect Healthcare Insurance Portability and Accountability Act, Personally Identifiable Information, and Criminal Justice Information Services data.*" Even though the department is considering a solution that will be maintained by the vendor, the vendor contract should include OIT's standards and best practices to implement and periodically assess the vendor's security controls. Please summarize the security experts the department will: (1) use during contract negotiations; (2) engage during system development to ensure the new solution is implemented with the appropriated security controls; and (3) assess periodically to certify compliance and adequate security.**

   As this solution is an OIT managed Enterprise Governance Committee (EGC) project, it is following the OIT Project Management Lifecycle and Gating process, to ensure OIT security experts are involved during every phase of the project. This includes the completion of the OIT Security Vendor Assessment, OIT Security Solution Assessment, creation and approval of the solution System Security Plan, and reception of an Authorization to Operate (ATO) Letter. The current development of the system was done through an OIT Contract and thus contains the Information Technology Provisions, received approval by the OIT IT Director, and passed OIT Executive Review.

   This will continue as system development persists with any work done on the system.

   1. Contract Negotiations: Even though CDPS will be the signing agency, the contract will be an OIT contract for ongoing hosting, support, and maintenance for the CCIB solution. This will require approval by the OIT IT Director and OIT Executive Review of the contract prior to its execution. During the OIT Executive Review, security experts will be engaged to review the contract. OIT Executive Review also ensures that the Information Technology Provisions are in place in the contract on any new contracts. The development and hosting vendor (Mainstream Technologies LLC) has a considerable amount of cybersecurity experience and expertise.

   2. System Development: The initial system development project has and will continue to adhere to the OIT Project Management Lifecycle. This includes several reviews by OIT Security, Compliance, and Technical personnel. These reviews result in the completion of the OIT Security Vendor Assessment, completion of the OIT Security Solution Assessment, creation and approval of the solution Architecture Plan, creation and approval of the solution System Security Plan, reception of an Authorization to Operate (ATO) Letter, as well as passage through the OIT Project Management Lifecycle gates.

   3. Periodic Assessment: Per the OIT Contract Provisions, the vendor is required to submit to an annual SOC2 Type II security audit. Along with this, the vendor is also contractually obligated to submit to periodic OIT Office of Information Security audits and penetration tests. Since solution development requires that a solution System Security Plan be created, it will require periodic reviews and updating per OIT Office of Information Security policies. The solution also requires continuous adherence to the FBI Criminal Justice Information Security (CJIS) standards in order to maintain a CJIS certification.

6. **The department estimates that the annual cost of the application and database servers is $5,388.48 and $19,286.88 respectively. Please provide more information regarding the estimates. Does the cost of the application and database servers include licenses? Is the department considering using virtual servers?**

   All servers are virtual servers in Mainstream's VMWare ESX environment. The difference between the Application server and the Database server is the cost of the SQL Server license. The database server includes the Service Provider License Agreement (SPLA) license for Microsoft SQL Server 2019. SQL Server is licensed per-processor in pairs, so that license is two pairs for 4 virtual CPUs total.

   The monthly costs all include prorated charges for CPU, memory, and storage on the Virtual Machine (VM) hosts, and also include backup, off-site disaster recovery, maintenance, patch management, etc. All but the Watchguard and Qualys appliances are Microsoft Windows servers; all Windows servers include an SPLA license for Microsoft Windows Server 2019. The Windows license a small proportion of the monthly cost, but there is no license fee for the CCIB software.