COLORADO

Office of State Planning & Budgeting

111 State Capitol
Denver, Colorado 80203

FY 2018-19

Supplemental Comeback Requests for Executive Branch Agencies

January 28, 2019

Office of State Planning and Budgeting
FY 2018-19 Budget Request Comeback Requests

Department:	Health Care Policy and Financing
Title:	S-9 Medicaid Enterprise Operations Comeback

	FY 2018-19 Appropriation	FY 2018-19 Budget Request	JBC Action	Comeback Request	Difference Between Action and Comeback Request
Total	**$74,179,480**	**$9,477,289**	**$0**	**$9,477,289**	**$9,477,289**
FTE	0.0	0.0	0.0	0.0	0.0
GF	$15,433,472	$433,424	$0	$433,424	$433,424
CF	$6,449,552	$433,713	$0	$433,713	$433,713
RF	$12,182	$0	$0	$0	$0
FF	$52,284,274	$8,610,152	$0	$8,610,152	$8,610,152

Summary of Initial Request:
The Department requests $9.5 million total funds, including $433,424 General Fund, to address operating and compliance issues for systems related to eligibility, enrollment, benefits authorization, and claims processing.

Committee Action:
The Committee delayed action so that feedback from representatives of the Governor's Office of Information Technology (OIT) could be obtained about the agency's role in the oversight of the Medicaid Enterprise.[1]

OSPB Comeback:
OSPB requests approval of the Department's S-9 Medicaid Enterprise Operations supplemental request as submitted.

OIT Roles and Responsibilities in Medicaid Enterprise Operations

The Governor's Office of Information Technology (OIT) works as a partner with the Department to implement modular services under the Medicaid Enterprise. Throughout the implementation of the Department's new claims processing and data management systems, the Department has followed the

---

[1] "Medicaid Enterprise" is a federal term that refers to the systems that enable efficient operations of the Medicaid and CHIP programs by supporting beneficiary eligibility, enrollment, care management, and other beneficiary-facing tools. These systems also serve provider enrollment and payment, benefits managements, data analytics and reporting, fraud and abuse detection, and provider electronic health record incentive payments. Medicaid Enterprise services are financed in large part with federal monies under the authority of the Social Security Act. Federal statute and regulations provides for enhanced federal financial participation (FFP) for operations at seventy-five percent and for design, development, implementation, and enhancement services at ninety percent.

OIT Enterprise Project Management Office (EPMO) process and reports to OIT monthly on the status of the projects, potential risks, and solutions. Additionally, the Department invited OIT representatives to be part of the RFP evaluation teams for project vendors. OIT performs an important role by performing an annual review of the vendors' compliance with the Colorado OIT Cyber Security policies. OIT performs a complete system security review when new vendors begin work to assure vendors perform required security scans, and gathers system diagrams from vendors for documentation to support compliance. OIT requires the vendor to provide a plan to resolve security issues when applicable. This complete Gate System Security Package must be reviewed, approved, and on file with OIT demonstrating compliance during implementation, including any remediation required with the authority to operation granted by OIT. In addition, vendors provide third party audit documents to assure that Colorado State Security Compliance is met ongoing through assessments (e.g., SOC 1 Type 2, SOC 2 Type 2 reports) at data centers, site locations and for various systems used by the vendor.

During the supplemental hearing on January 17, 2019, the Joint Budget Committee asked why the claims processing system, referred to as the Medicaid Management Information System (MMIS), was not under the authority of OIT. That decision was based on requirements from the federal Centers for Medicare and Medicaid Services (CMS). Federal law requires each state to designate a single state agency to administer or supervise the administration of its Medicaid program. The Department of Health Care Policy and Financing is Colorado's designated state Medicaid agency. In a letter from CMS dated January 15, 2009, the Department was informed that to receive the enhanced federal match rates, the MMIS must be under the direct control of the state Medicaid Director and the Department as the single state Medicaid agency. CMS holds the state Medicaid agency accountable for federal funds invested in the procurement, acquisition, and development of the MMIS. Enhanced federal matching funds cannot be leveraged through OIT. Based on the current operational structure with the MMIS being under the Department's direct authority, the state funding saved in FY 2018-19 by leveraging enhanced federal funding is approximately $12.7 million. If the authority is transferred to OIT and enhanced federal funding cannot be obtained, the state's contribution for these systems would increase by at least this amount in future fiscal years.

The Department believes that it is appropriate that the MMIS and associated Medicaid Enterprise systems remain under the control of the Department, with OIT supporting Department efforts. The Medicaid program is constantly changing and continues to become increasingly complex. Implementation of programmatic changes requires detailed policy work to happen in conjunction with changes to IT systems to ensure prompt and correct implementation. This type of collaboration requires dedicated staff who understand Medicaid policy as well as the technology associated with fundamental operational activity such as claims payment and provider enrollment. For these reasons, administration of the Medicaid Enterprise operations by the State Medicaid Agency is more efficient, economical, and effective because of the Department's expertise in Medicaid policy and its accountability for implementing requirements of the Medicaid program.

Role of the Joint Technology Committee

The Department frequently receives questions about the oversight role of the Governor's Office of Information Technology (OIT) and the Joint Technology Committee (JTC) regarding components of the Medicaid Enterprise operations. Although the components of the Medicaid Enterprise operations involve information technology, the Department emphasizes that it is purchasing business services for

Medicaid policy implementation and management from vendors, rather than standalone IT systems. Vendors determine how they can deliver those services which can include solutions using technology.

For example, the Department is contracting with a vendor to process and report on medical claims while also assisting the Department and providers with customer service issues. The vendor decides on the specific technology solution needed to meet the service requirements. Because these contracts are focused on the purchase of these services, as opposed to the purchase of IT systems, the requests for funding are submitted through the operating budget to the Joint Budget Committee (JBC), rather than through the JTC.

The Department and the Governor's Office recognize that there is a substantial information technology component of these contracts and that there may be benefits of additional oversight from the Joint Technology Committee. Going forward, the JBC will have an opportunity, including review of the Department's FY 2019-20 decision item related to Medicaid Enterprise Operations at Figure Setting, to consider whether these expenditures are more appropriately appropriated as capital construction funding as opposed to operating. If the decision is made that these expenditures should be made from capital construction appropriations, the Department would adjust future budget submissions accordingly.

At present, however, the supplemental funding issues identified are urgent and require prompt action from the JBC to prevent a significant loss of federal funds.

Review of Supplemental Funding Needs

The Department requested supplemental funding to address several critical needs related to its Medicaid Enterprise operations. It was widely known that the Department experienced significant challenges when implementing the new Medicaid Enterprise Services. The Department is unable to continue critical operations without supplemental funding in FY 2018-19.

The Medicaid Enterprise operations must be formally certified by the Centers for Medicare and Medicaid Services (CMS), which will enable the State to access enhanced federal financial participation (FFP) at the rate of 75 percent for operations. Without certification, the FFP matching rate would be limited to 50 percent and would result in a significant increase to the General Fund and other state funding source obligations. The Department experienced several unforeseen contingencies that must be addressed prior to system certification and results in the need for additional funding. Transition difficulties delayed certification and funding to assist with CMS certification has been exhausted.

The remaining funding requested as a supplemental adjustment is to address concerns affecting providers and members resulting from the transition to the new MMIS and Fiscal Agent. As part of the request, the Department requested funding to continue several contracted positions to ensure that calls for billing issues are answered timely and claims are processed timely; implement software to improve billing; address needs related to evolving federal requirements and stakeholder feedback in the development of a new care and case management and needs assessment tool. If the supplemental request is not approved these resources and operations cannot be continued and timely payment of providers is at risk, negatively impacting providers, and ultimately members.

Office of State Planning and Budgeting
FY 2018-19 Supplemental Comeback Requests

Department:	Department of Public Safety
Title:	S-02, BA-02 Safe2Tell Communications Officer Transfer

	FY 2018-19 Appropriation	FY 2018-19 Budget Request	JBC Action	Comeback Request	Difference Between Action and Comeback Request
Total	**$41,370,360**	**$27,303**	**$0**	**$27,303**	$27,303
FTE	143.8	0.0	0.0	0.0	0.0
GF	$7,780,881	$44,424	$17,121	$27,303	$27,303
CF	$29,439,340	$0	$0	$0	$0
RF	$3,162,287	($17,121)	($17,121)	$0	$0
FF	$987,852	$0	$0	$0	$0

Summary of Initial Request:

The Department requested funding for an upgraded phone system to manage call volume efficiently, and analytical software to provide the Safe2Tell unit with critical information to proactively identify and investigate school-related threats. This technology is essential to implement the Department's FY 2018-19 transfer of Safe2Tell dispatching services from the Colorado State Patrol (CSP) to the Watch Center within the Division of Homeland Security and Emergency Management's Office of Prevention and Security (Colorado Information Analysis Center).

Committee Action:

The Committee denied the Department's FY 2018-19 request for additional technology based upon JBC staff's recommendation. The following reasons were outlined in the staff recommendation:

- JBC staff did not believe the request met criteria for supplemental funding.
- There were concerns regarding the legislative intent of the Safe2Tell program.
- JBC staff expressed concern with maintaining anonymity of reporting parties.
- JBC staff did not believe that denying the supplemental would result in service disruption in the current year.

OSPB Comeback:

The Office of State Planning and Budgeting respectfully requests that the JBC approve the Department's request for the upgraded phone system, Dataminr software, and Babel Street software. Each bullet point above is addressed in the sections below.

Supplemental Criteria

The items in the supplemental request were identified when the Department began working with stakeholders, such as the Colorado State Patrol and the Attorney General's Office, to develop the implementation plan to effectively meet the needs of integrating the Safe2Tell program with the Watch Center in the first quarter of the fiscal year. Developing this plan gave the Department the opportunity

to conduct a thorough needs assessment to ensure a successful transition of the program from CSP to the Watch Center. Therefore, the requested items reflect new data that were not available previously.

Legislative Intent
Included in the supplemental hearing document is the following:

> *The Safe2Tell program was set up to be a **reactive**, confidential tip line. While the statute does direct law enforcement agencies to investigate, staff believes that the introduction of this software adds new components of proactive investigation, and presents some concerns to staff around privacy, confidentiality, and the statutory intent of the program.*

The Safe2Tell program was created following the tragic Columbine High School shooting. The Columbine Commission's Report recommended creating "an anonymous venue for parents, students, teachers, school administrators and law enforcement to share information," which became the Safe2Tell program. The Safe2Tell statute's legislative declaration specifically states that the intention of the program is to provide

> "... a readily accessible tool that allows students and the community to easily provide anonymous information about unsafe, potentially harmful, dangerous, violent, or criminal activities in schools, or the threat of these activities, to appropriate law enforcement and public safety agencies and school officials…[and]…the ability to anonymously report information about unsafe, potentially harmful, dangerous, violent, or criminal activities in schools before or after they have occurred [which] is critical in reducing, responding to, and recovering from these types of events in schools."

The Department believes the most important aspect of the legislative intent is preventing another tragedy like Columbine from happening again, which requires a proactive approach. While the Safe2Tell program does react to tips, the program's mission is largely proactive in nature. The social media monitoring is intended to help confirm threats, identify reported suspects as well as new threats to schools. In other words, the software will help the program react better, faster, and smarter by applying a proactive approach to investigating threats and preventing tragedy.

Preserving Privacy and Anonymity
The Department has the appropriate safeguards in place to preserve privacy. The Safe2Tell statute requires anonymity, and the Watch Center is committed to maintaining the anonymity of the reporting party, unless they voluntarily disclose their identity *and* verify that they are willing to be identified, which is the statutory requirement. The requested telephone upgrades and software will not compromise these protections.

As part of the Colorado Information Analysis Center, the Watch Center has a comprehensive privacy policy to prevent the inappropriate collection, use, and release of personal information including the privacy of personal behavior, communications and data. The privacy policy also protects civil rights, particularly First Amendment rights.

The sheer volume of social media content requires analytical tools to analyze threats associated with social media effectively and efficiently. This is of particular concern with the Safe2Tell program for the following reasons:

- Students often communicate via social media, including with the Safe2Tell program.
- About half of the threats made against schools since the Parkland shooting came from social media.
- One study of averted school shootings found that more than half (29 out of 51) of the plots studied were discovered by the shooters' peers, and perpetrators often directly told someone of their plans/threats. In many cases, the perpetrators talked about their plans on social media.
- Law enforcement and school administrators in Colorado indicate they are increasingly dealing with threats that often spread over social-media platforms, causing consternation among children and parents.
- If there is an incident involving a school, information about the unfolding incident is often posted on social media, giving the analysts the ability to forward critical information to responding units.

The use of social media monitoring software is consistent with the Department's privacy policy. The requested analytical software links directly with publicly available social media feeds. The systems do not look at private messages, private accounts, or private group postings. The requested tools simply aggregate publically available, open source data and provide sophisticated search tools to improve the effectiveness and efficiency of social media analysis. Without the requested tools, the only alternative involves a manual search of social media and data collection that will inevitably delay or prohibit the process of information collection.

Furthermore, the upgraded phone system will not undermine the anonymity of the reporting party. Even though the request did mention caller-ID, the phone system must serve the entire Watch Center. The caller-ID function is always disabled for calls to the Safe2Tell line.

Impacts in the Current Year
The current Watch Center phone system has limited capacity and does not have the ability to receive multiple calls simultaneously on one line. The requested upgrade will add telephone units and lines to the Watch Center for the Safe2Tell program to manage an expected increase in call volume.

JBC staff calculated the average monthly call volume as if it were evenly distributed throughout the year. It is important to note that the actual call volume varies significantly depending on the month, and call volume average does not account for seasonality. While the existing phone system is sufficient to handle call volume in July, it is not equipped to manage call volume during the school session. The potential ramifications of missing one of these calls could have life threatening consequences. When there is an evolving incident at a school, there is potential to overwhelm local dispatch centers. When this occurs, calls move to Safe2Tell as the next known reporting entity. We expect the workload and call volume for the Watch Center to increase over time. For example, Safe2Tell reports increased 76 percent from FY 2016-17 to FY 2017-18. Furthermore, based upon year-to-date figures, we expect the program to increase by at least 20 percent from FY 2017-18 to FY 2018-19.

Conclusion
One primary reason the Safe2Tell call responsibilities transitioned to the Watch Center is that CSP dispatch could not provide the desired level of analytical support to the program. The Department believes the Watch Center is the best place for the Safe2Tell program; however, social media monitoring

software will enhance the Watch Center's ability to identify threats proactively. The requested tools will monitor open source data in real time, thus providing the opportunity to prevent an incident or gather crucial intelligence about an unfolding or planned incident. Furthermore, the telephone system upgrade is crucial for capacity building as the Safe2Tell program continues to experience growth.

For the reasons stated above, the Department believes the Safe2Tell program request does meet criteria for supplemental funding. Additionally, the Safe2Tell program aligns with the legislative intent, which requires both reactive and proactive measures, while simultaneously ensuring the appropriate safeguards are in place to preserve anonymity of reporting parties.

Office of State Planning and Budgeting
FY 2018-19 Supplemental Comeback Request

Department:	Transportation
Title:	Multimodal Transportation Options Fund

	FY 2018-19 Appropriation	FY 2018-19 Supplemental Request	JBC Action	Comeback Request	Difference Between Action and Comeback Request
Total	**$0**	**$0**	**$0**	**$0**	**$0**
GF	$0	$0	$0	$0	$0
CF	$0	$71,750,000	$31,500,000	$71,750,000	$40,250,000
RF	$0	$0	$0	$0	$0
FF	$0	$0	$0	$0	$0

Summary of Initial Request:

In May 2018, the Colorado General Assembly passed Senate Bill (SB) 18-001 and the Governor signed it. The legislation allocated $71.75 million for fiscal year (FY) 2018-19 to the newly created Multimodal Tansportation Options Fund (MTOF). A drafting error in the legislation seems to have prevented the allocation from being legislatively appropriated. Since the legislation passed at the end of the 2018 legislative session and was signed after the Long Bill, there was no opportunity for CDOT to seek an appropriation from the legislature for funds in the MTOF. In January 2019, the Department requested a supplemental appropriation of $71.75 million from the MTOF.

Committee Action:

Joint Budget Committee (JBC) staff recommended the committee approve an appropriation of $31.5 million from the MTOF for FY 2018-19, and recommended that this appropriatoin remain available for expenditure until the close of FY 2022-23. The JBC voted to approve the staff recommendation.

OSPB Comeback:

The Department and stakeholders involved in approving the $71.75 million for multimodal funding believe that the full amount should be available to the Department pursuant to the intent of SB18-001.

Pursuant to SB 18-001, 85 percent of the funding from the MTOF passes through the department and is allocated to local multimodal projects. Since most of the funding in the MTOF is this pass-through funding, local governments statewide will benefit from the allocation of multimodal funds. The department has worked over the last eight months with local government, transit organizations, rural transit providers, and a variety of other stakeholders to develop a process and plan for distribution of these SB 18-001 MTOF funds. Local multimodal projects will be delayed if the entire $71.75 million is not allocated pursuant to the SB 18-001 langauge. The department respectfully requests access to the full $71.75 million allocated to the MTOF for multimodal projects.

Office of State Planning and Budgeting
FY 2018-19 Supplemental Comeback Request

Department:	Transportation
Title:	Southwest Chief Rail

	FY 2018-19 Appropriation	FY 2018-19 Supplemental Request	JBC Action	Comeback Request	Difference Between Action and Comeback Request
Total	$0	$0	$0	$0	$0
GF	$0	$0	$0	$0	$0
CF	$0	$1,380,447	$1,380,447	$1,568,591	$188,144
RF	$0	$0	$0	$0	$0
FF	$0	$0	$0	$0	$0

Summary of Initial Request:

In May 2018, the Colorado General Assembly passed Senate Bill (SB) 18-001 and the Governor signed it. The legislation allocated $2.5 million for fiscal year (FY) 2018-19 to the Southwest Chief and Front Range Rail Commission (Commission). Since the legislation passed at the end of the 2018 legislative session and was signed after the Long Bill, there was no opportunity for CDOT to seek an appropriation from the legislature for these funds.

In September 2018, the Department requested a 1331 supplemental for the full $2.5 million allocated by SB18-001. The Joint Budget Committee (JBC) partially approved the 1331 supplemental in September 2018 for $931,409. In January 2019, the Department requested another $1.38 million and rollforward authority.

Committee Action:

The JBC approved the department's request for an appropriation of $1,380,447 million from the Southwest Chief Rail Line Economic Development, Rural Tourism, and Infrastructure Repair and Maintenance Fund (SW Chief Fund).

OSPB Comeback:

The department's request for $1,380,447 was based on expected Commission expenditures from the SW Chief Fund. However, this amount is $188,144 short of the full $2.5 million allocated to the fund by SB 18-001. The Department believes that the full $2.5 million allocated should be available pursuant to the intent of SB18-001. This comeback request is for the remainder of the $2.5 million that has not yet been allocated.