Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Memorandum

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

February 15, 2019

TO: Joint Technology Committee Members

FROM: Jean Billingsley, Senior Research Analyst, 303-866-2357
Joint Technology Committee (JTC) Staff

SUBJECT: JTC Staff Analysis of JBC-Referred FY 2019-20 Budget Request
Colorado Governor's Office of Technology
R-02 Securing IT Operations

Summary of Request

The Governor's Office of Information Technology (OIT) is requesting $11.8 million and 9.0 full-time employees (FTEs) in FY 2019-20 for four IT security operations projects and to accelerate its existing Security Colorado initiative, consisting of seven projects.

Reason for Referral

This memorandum responds to the January 4, 2019, letter from the Joint Budget Committee (JBC) to provide a technical review of the OIT FY 2019-20 Securing IT Operations budget request (request).

Staff Analysis

Staff found that the justification, cost estimates, and research that OIT provided to support its FY 2019-20 operating budget request is thorough and detailed. Staff recognizes that assessing technology risks, including identifying potential security threats (i.e., computer viruses) and vulnerabilities (i.e., outdated server patches) has become a critical function for the state. IT security assessments may lead to a decision to mitigate a security risk by implementing security controls. Even so, the decision to mitigate a risk depends on the options and the tolerance level of the organization to accept a security risk. On that basis, OIT says that this request addresses all of its identified needs, and it has no plans to procure additional IT security software or services in FY 2019-20.

Specifically, the request addresses gaps discovered after the Colorado Department of Transportation (CDOT) security incident, and mitigates cloud solution security vulnerabilities with additional FTEs,

term-limited contractors, software, and hardware by creating four IT security projects and accelerating the existing seven Secure Colorado projects. For each additional FTE and contractor position needed for the security projects, OIT provides a description of the role, and corresponding role responsibilities, along with estimated hours for each role. OIT also provides itemized cost estimates, milestones, planned end dates, and details for each of the projects described in the request. Finally, OIT explains the need for security personnel training, security staff salary increases, and the creation of essential documentation.

Request Details

OIT explains that the request will mitigate security risks by adding or improving its existing IT security human resources, processes, technology, and services. In the request, OIT references the security incident that occurred at CDOT in February 2018. Roughly half of the department's computers were attacked by ransomware, which is malware that infects a computer, and restricts user access, usually until a ransom is paid to unlock the system to possibly decrypt a system's data.

Justification. OIT provides the justifications described below for its four IT security operations projects.

East-west network traffic. OIT explains that updating the east-west network traffic will improve securing applications that communicate with each other at the state data centers. OIT says that the CDOT incident may have been contained if the east-west traffic were more secure.

Public cloud. OIT explains that it supports and manages technical solutions on site, but it cannot adequately manage additional public cloud solutions within current resources. As of January 2019, OIT has 149 cloud projects or solutions it supports, and it has received a total of 273 cloud requests since March 2018. OIT says the limitation in resources became particularly evident after the CDOT security incident.

Identity and access management. The request provides resources to accelerate cloud integration with privileged account management to prevent inappropriate administrative access, such as inadvertently granting elevated permissions, or a malicious bad actor obtaining administrative access. The request completes the statewide implementation of securing integration with four high-priority systems, such as the state's new human resource system, HRWorks.

OIT infrastructure security teams. The request adjusts salaries for the security staff. OIT says that its security department, comparable to regional and national IT security attrition trends, experienced approximately a 65 percent turnover in 2016 and 2017, compared to a 16 percent turnover in the entire OIT organization. OIT explains that it is concerned about retaining its security operations staff, who are the front-line defense against cyber attacks, and it recommends adjusting salaries in these hard-to-fill positions.

OIT provides the following justifications for accelerating its existing Secure Colorado initiative. OIT began Secure Colorado in 2012 to support strategic decisions that protect the state's information assets. OIT explains that without the funding in the request, some of its Secure Colorado projects may not be

completed until 2023, or later. However, with the funding in the request, all the Secure Colorado projects will have a planned end date of June 2020 or sooner.

OIT describes the Secure Colorado projects as the: *(1) Logging Repository Storage* project, which will prevent attacks, and will be used for security forensics after a security incident; (2) *Role Based Access* project and *Privileged Access Management* project, which will grant and manage user permissions according to a user's job, along with added controls for privileged access; (3) *Two-Factor Authentication* project, which will add another layer for authenticating access to a state system; (4) *Agency Firewalls* project, which will upgrade the firewall with significant security enhancements; (5) *Server and Deskside Endpoint Management* project, which will implement a statewide tool instead of the variety of tools being used at the agencies currently; and (6) *Staff Augmentation* project, which will hire temporary resources to perform proactive assessments while existing personnel increase the completion of audit activities.

Itemized cost information. OIT provided estimates for each security project (see Appendix B, FY 2019-20 Securing IT Operations Request Itemization). $6.0 million of the request is for the four IT security operations projects. Approximately 35 percent, or $4.1 million, of the FY 2019-20 request is to accelerate the existing Secure Colorado projects. Secure Colorado funding has increased each fiscal year as follows:

- $4.1 million in FY 2015-16;
- $5.1 million in FY 2016-17;
- $8.1 million in FY 2017-18; and
- $7.8 million in FY 2018-19.

Future operating expenses. Departments will see an increase in the OIT reappropriation cost allocation in FY 2019-20 ranging from $2.5 million, charged to the Colorado Department of Corrections, to $0.01 million, charged to the Colorado Department of the Treasury (see Appendix A: OIT Reappropriation to the Departments).

Cost estimates and research. OIT used market research in order to determine the costs and the recommended tools. For each of the existing Secure Colorado projects, OIT gave JTC staff a milestone list of project deliverables, such as testing, developing a proof-of-concept, and publishing a request for information. OIT also provided the status of its existing Secure Colorado projects.

Program Information

The mission of OIT's Office of Information Security is to develop and manage the state's information security program. OIT directly aligns its goals and objectives with the National Strategy to Secure Cyberspace, along with establishing partnerships with federal, state, local, and private sector experts. In 2012, the OIT Chief Information Security Officer developed the Secure Colorado initiative with the help of the Colorado Information Security Advisory Board. In 2015, the Colorado Information Security Advisory Board reviewed Secure Colorado, and found its direction and priorities to be relevant, appropriate, and sound.

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, as outlined in the JTC Staff Analysis section;
- recommend the request to the JBC for funding with concerns; or
- not recommend the request for funding with concerns.

Appendix A
OIT Reappropriation to the Departments

Department	FY 2019-20	FY 2020-21
Agriculture	$115,300	$49,238
Corrections	$2,471,321	$1,055,356
Education	$236,799	$101,123
Governor's Office	$55,161	$23,556
Healthcare Policy and Financing	$180,748	$77,187
Higher Education	$54,369	$23,218
Human Services	$1,952,949	$833,989
Judicial	$1,836,297	$784,174
Labor and Employment	$506,371	$216,241
Law	$186,947	$79,834
Local Affairs	$69,075	$29,498
Military and Veterans Affairs	$31,422	$13,418
Natural Resources	$577,094	$246,443
Personnel and Administration	$167,098	$71,358
Public Health and Environment	$526,055	$224,647
Public Safety	$712,408	$304,228
Regulatory Agencies	$226,512	$96,730
Revenue	$567,895	$242,515
State	$54,369	$23,218
Transportation	$1,316,275	$562,104
Treasury	$13,024	$5,562
TOTALS	**$ 11,857,490**	**$ 5,063,637**

Source: Governor's Office of Technology FY 2019-20 Operating Budget Request.

Appendix B
FY 2019-20 Securing IT Operations Request Itemization

OIT Securing IT Operations Requested Allocations of Funds

Description	FY 2019-20	FY 2020-21 and Out-years
Network Upgrades at Agencies *improve network, remote, web access*	$1,500,000	$0
Palo-Alto Firewall Upgrades *added capabilities to create security rules*	$1,285,000	$231,300
1.0 FTE Network Engineer *design, implement, test, vendor management*	$140,653	$140,653
Salary Adjustments *address existing attrition issues*	$407,000	$407,000
East-West Network Traffic:	**$3,332,653**	**$778,953**
2.0 FTE Cloud Architects *design cloud solutions-emphasis on security*	$267,189	$267,189
2.0 FTE Cloud Engineers *implement / change environments*	$267,189	$267,189
1.0 FTE Security Program Manager *security expert for large-scale security projects*	$153,951	$153,951
One-time Onboarding Costs *personal computer, furniture*	$50,876	$8,549
Public Cloud:	**$739,205**	**$696,878**
2.0 FTE Senior Analyst *manage identity services and user access*	$307,901	$307,901
Identity Analytics and Risk Intelligence *solution for identity and access management*	$361,000	$1,000
Data and Access Governance *solution granting access to sensitive data*	$730,000	$370,000
Cloud Access Security Broker *tool to automate access to data in the cloud*	$492,000	$402,000
Identity and Access Management:	**$1,890,901**	**$1,080,901**
1.0 FTE Security Engineer *execute cloud security strategy and best practices*	$126,535	$126,535
Technical Training and Development *security certifications two leads from each infrastructure group for*	$180,000	$0
Incident Response and Management Training *training to address gap discovered after CDOT incident*	$105,000	$0
End-to-End Monitoring and Logging *real-time visibility between the user device and the application*	$1,175,000	$900,000
Standard, and Operational Sustainability Documentation *two contractors for one year to document infrastructure standards*	$180,000	$0
OIT Infrastructure Security Teams:	**$1,766,535**	**$1,026,535**
Logging Repository Storage	$250,000	$90,000
Role-Based Access Controls	$650,000	$0
Privileged Access Management	$607,350	$44,523
Two-Factor Authentication	$335,846	$155,846
Upgrade Agency Firewalls	$975,000	$45,000
Server and Deskside Endpoint Management	$1,145,000	$1,145,000
Staff Augmentation	$165,000	$0
Existing Secure Colorado Projects:	**$4,128,196**	**$1,480,369**
Grand Total:	**$11,857,490**	**$5,063,636**

Source: Governor's Office of Technology FY 2019-20 Operating Budget Request.