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

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-11 Entire State Cybersecurity Approach Program

Summary of Request

The Colorado Department of Public Safety (DPS) is requesting $385,943 General Fund and 3.0 FTE in FY 2022-23 and $364,943 and 3.0 FTE in FY 2023-24 and ongoing to create Cybersecurity Technical Assistance Group within the Colorado Information Analysis Center. The Joint Budget Committee (JBC) has asked the Joint Technology Committee (JTC) to provide a technical review of this request.

Request Details

The Cybersecurity Subcommittee of the Homeland Security and All-Hazards Senior Advisory Committee, created in Section 24-33.5-1614, C.R.S., has recommended implementing a "Whole of State" cybersecurity approach to help raise the security posture of Colorado. As part of this approach, the subcommittee has recommended the creation of a Cybersecurity Technical Assistance Group. More information about the work of the subcommittee and its recommendations can be found here: https://dhsem.colorado.gov/dhsem/councils-and-committees/hsac/hsac-subcommittee-information/cybersecurity-hsac-subcommittee.

The requested 3.0 FTE that will form the Cybersecurity Technical Assistance Group will assist local jurisdictions and state agencies in mitigating, protecting against, planning for, responding to, and recovering from cybersecurity incidents. This work will include helping local governments throughout the state develop sound processes to procure and operate IT assets with basic security awareness and practices. Key areas of focus for the group will include:

- supporting outreach and training;
- assisting in developing policy and compliance attainment;
- designing and exercising incident response plans;

- supporting various assessment activities in conjunction with the private sector;
- engaging state and federal partners; and
- providing support to identify and reduce cyber risk.

According to the department, the Governor's Office of Information Technology (OIT) supports this proposal, though the program will be distinct from current OIT cybersecurity initiatives through Secure Colorado.

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 describe the department's current and anticipated collaboration with OIT on Secure Colorado and other cybersecurity efforts in the state, along with the department's collaboration with various other entities engaged in this effort (National Cybersecurity Center, MS-ISAC, etc.).**

   DPS has, and will continue to have, a very close partnership with the Governor's Office of Information Technology (OIT) in the cybersecurity domain, including Secure Colorado. The current partnership with OIT includes sponsoring security clearances for key staff; providing secure space for classified information sharing; sharing unclassified threat information; partnering with OIT, FBI, DHS, Colorado National Guard, and other agencies in the cybersecurity domain; developing cyber response plans for state systems, responding to state cyber incidents as necessary (CDOT ransomware incident); joint participation in the Cybersecurity Council and the Homeland Security Senior Advisory Committee; and a variety of other related activities.

   The collaboration will be enhanced by R-11, which will increase the overall cybersecurity posture of Colorado. Future collaborative efforts include enhanced partnerships external to the state in training, knowledge-sharing, and creating and implementing a cybersecurity assistance group within the Colorado Information Analysis Center (CIAC). This new group's mission will address growing cybersecurity concerns across the state, particularly with local and tribal governments and other critical infrastructure providers. This group will assist local jurisdictions and other critical infrastructure providers to develop and implement tools to prevent, mitigate, plan for, respond to, and recover from cyber security incidents, e.g. develop and enroll local and tribal governments in cyber incident response mutual aid agreements.

DPS will further collaborate with the National Cybersecurity Center and MS-ISAC to help establish baseline local government cyber risk profiles and comprehensive support to adopt best practices for their communities. These efforts will decrease the likelihood of successful cyberattacks and improve recovery from those attacks that cannot be prevented.

Working in collaboration with OIT, the National Cybersecurity Center, MS-ISAC, local and tribal governments and our federal partners, the DPS lead Cybersecurity Program will support the following goals of the Homeland Security Senior Advisory Committee's Cyber Subcommittee's statewide goals:

● Partnerships – enter into partnership between public and private sectors; between public sector entities at all levels of the state; and with higher education and K-12 entities to maximize resources and efficiencies to move cybersecurity goals forward.

● Cyber Reserves – develop a formal incident response team to assist jurisdictions that become victims of cyberattacks.

● Cyber Range – coordinate with the National Cybersecurity Center to utilize the Cyber Range to deliver training to state and local government cybersecurity workforce.

● Cyber Support Center – support local and tribal governments with technical support, best practices, policy development, and incident response and recovery.

● Threat Intelligence & Community Collaboration – provide relevant threat intelligence. The cybersecurity program will continue the strong partnership between PIT and the CIAC and better serve local and tribal governments and other critical infrastructure providers.