Department of Information Technology
Fiscal Year 2022 Operating Budget
Response to Department of Legislative Services Analysis

Senate Budget and Taxation Committee

Public Safety, Transportation and Environment Subcommittee

The Honorable Cory V. McCray, Chair

March 5, 2021

House Appropriations Committee

Public Safety and Administration Subcommittee

The Honorable Keith E. Haynes, Chair

March 5, 2021

The Department of Information Technology (DoIT) appreciates the opportunity to respond to the Department of Legislative Services' (DLS) analysis of the Office of the Secretary's budget.

The DLS Analysis focuses on three key observations, which include the increase in remote work through shared services IT support, the continuing cybersecurity challenges, and the agencies that appear to be struggling with Major Information Technology Development Projects (MITDP). The following testimony addresses the requests for comments in the analysis, as well as the DLS recommendations.

Requests for Comment

1. **Major IT Project Recommendations and Discussion**
   - **MDH's COVID-LINK Oversight: The department should be prepared to brief the committees on the status of this project.**

     In September 2020, the DoIT Secretary deemed COVID LINK as an Out of Cycle (OOC) MITDP. The project is being implemented on an emergency schedule therefore, the project team is pivoting to meet changing demands.

     The COVID-LINK MITDP project scope includes MDH's contact tracing systems. Contact tracing is the process by which health officials identify persons with infectious diseases and other persons with whom they have come in contact. MDH performed an initial product rollout in 2020. MDH has recently undertaken a second stage of system enhancements to respond to rapidly evolving needs arising from the late 2020 surge in cases and the discovery of COVID variants, and an ITPR that reflects these new enhancements is forthcoming.

   - **Maryland State Department of Education (MSDE) and Interagency Commission on School Construction (IAC) Business Management System (BMS): DoIT should be prepared to brief the committees on the BMS project delays, risks, and its plans to ensure success for this project.**

     Due to a lack of participation from the market, the IAC withdrew its request for proposal (RFP) for the replacement of the BMS in November 2020. Since that time, the IAC has been working collaboratively with DoIT to amend the requirements of the solicitation and its subsequent reissuance. The IAC anticipates BPW award, assuming no further delays, within the first quarter of FY2022.

     The implementation of the new BMS will relieve IAC of the manual accounting processes that currently take place and allow the agency to achieve cost containment and process efficiencies. The IAC will continue using legacy systems and workflows until the procurement and subsequent BPW award is completed and the new BMS is implemented.
     DoIT will continue its oversight engagement with the agency/project team to monitor the project's progress and proactively identify any concerns or issues as they arise to ensure prompt resolution.

   - **Comptroller's Office ITS: It is recommended that this narrative be adopted again for fiscal 2022 in the Comptroller's Office budget.**

DoIT concurs with this recommendation.

- **DHS Shared Human Services Platform or Maryland Total Human-services Integrated Network (MD THINK): In the DHS Administration budget, the Department of Legislative Services (DLS) is recommending narrative requesting periodic project updates and restrictive language requiring a cost estimate report. DoIT should be prepared to brief the committees on actions taken to minimize the risks associated with implementing so many large components over a short period of time and process changes to ensure that spending data reported with the budget is accurate.**

  DoIT oversight and IV&V continue to monitor performance and address any concerns/risks for MDTHINK. DoIT and DHS engage in weekly collaboration meetings to resolve and mitigate concerns/risks accordingly. Additionally, DoIT has assumed a more active role in financial oversight for MDTHINK, which includes analyzing the monthly spend plan provided by DHS, developing projected spend and burn rates for the remainder of the fiscal year, requesting backup detail to spend, and reviewing the quarterly DHS Joint Chairmen's Reports (JCR) submitted. All analyses and feedback are provided to DHS in an effort to ensure consistency and transparency between the two agencies.

- **Department of Public Safety and Correctional Services (DPSCS) Computerized Criminal History Replacement: DoIT should brief the committees on the delays that led to this loss of federal funds and steps taken to improve DPSCS's ability to implement major IT projects.**

  The Computerized Criminal History (CCH) replacement project encountered numerous project delays leading up to the issuance of the RFP, resulting in the reversion of federal grant funds. These delays have been attributed to the RFP development, review, issuance, and changes to technical requirements. DPSCS Procurement has kept DoIT apprised of changes to the procurement and provided assurances that an award recommendation will be forthcoming in the fourth quarter of FY2021.

  DoIT will continue its oversight engagement with DPSCS to monitor the project's progress and proactively identify any concerns or issues that may threaten the project's implementation.

- **State Board of Elections (SBE) Agency Election Management System (AEMS) and Pollbook Project: In the SBE budget, DLS recommends that narrative requiring periodic status reports be adopted again. DLS recommends narrative concerning local cost sharing in the SBE analysis.**

  DoIT concurs with this recommendation.

Issues

1. **Cybersecurity Challenges Continue Unabated**
   - **The department should brief the committees on the role of the new SCISO. MCCC has now been operating for over a year. DoIT should be prepared to brief the committees on how MCCC has improved the State's coordination of and response to cybersecurity threats.**

     The role of the SCISO is specifically defined in Executive Order 01.01.2019.07; however, the SCISO's role is to lead the Office of Security Management (OSM). The OSM, located within DoIT, is responsible for the direction, coordination, and implementation of the overall cybersecurity strategy and policy for all State agencies in the Executive Branch.

     Over the last twelve months, cybersecurity challenges across several environments and criteria have been presented - both anticipated and unanticipated or unforeseeable. The SCISO, the OSM, and DoIT have addressed these challenges effectively and efficiently through implementation of a series of actions necessary to define the parameters of cybersecurity actions and responses that maximize the viability of the tools and resources available.

     The members of the Maryland Cybersecurity Coordinating Council (MCCC) have raised several concerns that the OSM worked to address. The first concern was limitations in the maryland.gov email system that prevented timely response to email-based threats. The OSM evaluated and implemented updates to the system that permitted threat-response from the 24/7 Security Operations Center (SOC) instead of the email support team, resulting in an immediate and substantive improvement in our ability to address phishing and malware attacks through the State's email system. This change was timely, as threat-actors shifted to using email delivery for the first stage of ransomware delivery.

The second concern identified was a lack of consistency in describing the phases and language around the Techniques, Tactics, and Procedures (TTPs) used by threat-actors. After consultation with experts, the OSM confirmed that our approach of using the MITRE ATT&CK framework to describe cyber-attacks was appropriate for the State. Using this framework creates consistency in describing both the TTPs and the remediations necessary to prevent the progression of cyber-attacks.

Regarding improvements to the State's cybersecurity response, 2020 began with a policy workshop facilitated by the National Governors Association (NGA). The workshop addressed updating our Statewide cyber-disruption plan emphasizing the response to large-scale disruptions, such as those caused by ransomware. The months following the workshop provided the OSM with several opportunities to validate the assumptions made during the cyber-disruption plan's development. The nature of these events and the organizations impacted allowed us to identify unanticipated gaps in cybersecurity consequence-management. While the plan adequately addressed the response to an event affecting a State entity, the OSM determined that one of the biggest challenges in responding to these events was a lack of clarity of authorities and responsibilities in edge cases, such as local health departments, county jails, and public school systems. The lessons learned in these responses are helping the OSM to develop a more comprehensive and effective cyber-disruption plan.

Because the reformulation of the written plan is heavily dependent on participation from units that are engaged in coronavirus response, the OSM has delayed this activity until the appropriate resources are available. This resource constraint has not prevented the plan from being communicated to key stakeholders. In fact, it has been used with success in several large-scale cyber-disruptions, including a large school-system and a private hospital system.

While not all cybersecurity risks can be removed entirely, we are confident that appropriate decisions have been made in protecting the State's assets. This is evidenced by the low number of disruptions impacting the Executive branch, and is more impressive when compared to other states.

- **To better understand cybersecurity threats and the State's response to these threats, DLS recommends narrative to request DoIT to submit a cybersecurity report.**

  DoIT concurs with this recommendation.

Operating Budget Recommended Actions

1. **Adopt the following narrative:**

   Review of State Cybersecurity: The committees are concerned about cybersecurity risks to State networks and systems. Maintaining the integrity, confidentiality, and accessibility of State networks is a challenge. The State has a decentralized information technology network that is commonly viewed as complicating cybersecurity defenses. The Office of Legislative Audits identified 33 cybersecurity findings in calendar 2020. These cybersecurity findings include vulnerable personally identifiable information, inadequate personnel controls, and inadequate technical controls. Adding to this challenge is an increased number of remote workers, which increased from less than 1% in January 2020 to almost 50% in January 2021. There are concerns that threats from cybercriminals are evolving to target remote workers. The Department of Information Technology (DoIT) should report to the committees on cybersecurity risks and the State's response to those risks. The report should include (1) recent audit findings, how the State has responded to these findings, and what needs to be done to reduce findings in future audits; (2) the role of the State Chief Information Security Officer (SCISO) and Maryland Cybersecurity Coordinating Council (MCCC) in addressing cybersecurity risks, including what has been achieved since the 2019 executive order creating SCISO and MCCC; (3) how remote work has increased risks and what the State's response is to those risks; and (4) how cybersecurity risks are evolving and how the State response will need to evolve to address those risks. The report should be submitted by November 19, 2021.

   DoIT concurs with this recommendation.