Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Acting Secretary

Department of Information Technology
Fiscal Year 2024 Operating Budget
Response to Department of Legislative Services Analysis

House Appropriations Committee

Public Safety and Administration Subcommittee

The Honorable Tony Bridges, Chair

February 16, 2023

Senate Budget and Taxation Committee

Education, Business and Administration Subcommittee

The Honorable Nancy J. King, Chair

February 20, 2023

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 two key observations, which include the increase in funding for Major Information Technology Development Projects (MITDP) and the comprehensive legislation restructuring cybersecurity that was enacted in 2022. The following testimony addresses the requests for comments in the analysis. DoIT concurs with all three operating budget recommendations in the DLS analysis.

<u>Performance Analysis: Managing for Results</u>

1. **<u>Cybersecutity</u>**

   DoIT should be prepared to brief the committees on its efforts to improve the share of employees compliant with cybersecurity awareness training.

   The DoIT Security Awareness Training Program provides a wide variety of cybersecurity training to State employees. The Office of Security Management (OSM) is responsible for bringing awareness to State employees and working as a partner with State agencies to enhance their cybersecurity awareness.

   DoIT continues to work with Agency Security Awareness Training Managers to enforce their responsibility to maintain accurate employee information in the Cybersecurity training platform, Infosec IQ. Additionally, all agency Security Awareness Managers continue to receive agency completion reports on a weekly basis to ensure the compliance of their agency. OSM held its first quarterly Security Awareness Training Summit on February 15th, where the focus was on cybersecurity training for specific agency job functions and monthly awareness training. All Agency Security Awareness Training Managers were encouraged to attend.

   The department should be prepared to discuss strategies to improve compliance with critical patches.

   Maintaining high rates of critical patch compliance, including that for system firmware, operating systems, and installed applications is fundamental for effective cybersecurity. Delivering those high rates of compliance is the obligation of information technology (IT) support organizations around the State. DoIT has taken several steps to improve the effectiveness of patching and vulnerability management for the systems subject to DoIT management services, including improved reporting, increased status communication, and a heightened focus on improved compliance outcomes. DoIT has realigned existing staff and will continue to build a dedicated team to specifically focus on tasks related to patching and vulnerability remediation within the DoIT Enterprise environment.

DoIT expects that the increased visibility of critical patch compliance effectiveness which will be provided through the new Endpoint Detection and Response (EDR) platform, combined with improved Statewide cybersecurity collaboration and the increasing centralization of cybersecurity services, will result in much higher rates of compliance throughout the State.

2. **Oversight of Major IT Projects**

No request for comment.

3. **Support Services for State Agencies**

DoIT should be prepared to brief the committees on the status of the workload and efficiency goals and indicators.

Over the last four years, DoIT has been fine tuning the implementation of Technology Business Management (TBM) in an effort to increase the transparency relating to the cost of providing IT services to our customers. These efforts include annually evaluating service consumption, rate setting and service-level agreements (SLAs) for services offered in the DoIT service catalog. A logical next step in that process would be to compare the services offered to those offered in the private sector to ensure DoIT's services are not only cost effective but also provide value. DoIT is in the process of soliciting a contractor to perform a comparison of DoIT IT service rates to the industry benchmarks, as well as develop performance metrics to measure workload and efficiency relating to DoIT IT services. Results are pending completion of a solicitation and subsequent engagement.

Issues

1. **Cybersecurity**

The department should be prepared to brief the budget committees on its plans to implement the new cybersecurity legislation.

As the DLS analysis mentions, the cybersecurity legislation passed in 2022 included three bills that enhanced state and local cybersecurity capabilities. To date, DoIT has already begun implementing various components of the legislation to include:

- Hired Director of State Cybersecuirty and Director of Local Cybersecurity.
- Established the Maryland Information Sharing and Analysis Center (MD-ISAC) to support collective defense.
- Created the Maryland Local Cybersecurity Collaborative (MLCC) in an effort to support local governments.
- Increased the Maryland Cybersecurity Coordinating Council (MCCC) membership and held two meetings.
- Issued cybersecurity incident reporting requirements for state and local governments.
- Aligned with the requirement to establish standards for reporting cybersecurity incidents, OSM launched the "Maryland Incident Reporting System," an online portal for reporting cybersecurity incidents directly to the Maryland Security Operations Center (SOC).
- Established guidelines for incident disclosure to the public.
- Hired a contractor to perform a capacity assessment that includes an analysis of both DoIT and OSM's ability to implement the legislation, as well as recommendations for the proposed structure and centralization of cybersecurity services.
- Implementation of a governance, risk and compliance (GRC) module.
- DoIT organized and hosted three Modernize Maryland Oversight Commission (MMOC) meetings. The Commission has voted on a chair, vice chair and a charter and has begun to organize working groups on numerous topics.

In addition to these initiatives, the fiscal year 2024 Governor's Allowance includes the addition of twenty cybersecurity positions that will allow OSM to take on initiatives such as the expansion of the SOC and MD-ISAC to all units of government and centralization of cybersecurity services.

2. Update on DPA Cybersecurity Spending

As with the fiscal 2023 DPA appropriations, DLS recommends committee narrative that outlines how these funds will be spent.

DoIT concurs with this recommendation.

3. **Remote Work Is Key to Having an Effective Government Workforce**

DoIT should be prepared to brief the committees on its efforts to have a safe and user-friendly remote workforce network.

Over the past year DoIT has been implementing and evaluating a stack of technologies through a proof of concept and pilot program aimed at delivering an improved user experience for a remote workforce, improved network and resource security, and improved administrative efficiencies while implementing a platform which could be leveraged Statewide and provide these capabilities to all agencies regardless of whether they are directly supported by DoIT Enterprise services. Unfortunately, this stack of technologies did not demonstrate any significant benefits over systems and operations already in place, and DoIT will not be expanding that pilot program or continuing the evaluation of that technology as configured.

However, in separate efforts DoIT began implementing a Statewide Endpoint Detection and Response (EDR) solution to help improve endpoint security, as well as implementing the foundational components of a Statewide Identity and Access Management (IAM) platform. These systems introduce core common Statewide capabilities to support the security and effectiveness of a remote workforce. In order to build on these, DoIT must evaluate other complementary technologies and products including a remote network access solution, and mobile device and user endpoint management solutions. Additionally, DoIT will evaluate and better understand how virtual desktop technology and third party Device as a Service (DaaS) offerings might best be leveraged at a Statewide level to better serve remote workforce needs for quick access to device and service provisioning.

4. **Vendor for OneStop Portal Files for Bankruptcy**

DoIT should be prepared to brief the committees on these questions.

- *To what extent does this bankruptcy increase costs or delay implementation of new components of DNR's OneStop Portal?*

  Due to a combination of factors, DNR and DoIT agreed that pivoting to the development of a new request for proposal (RFP) was the appropriate path forward for DNRs OneStop Portal. These factors included the Chapter 11

Bankruptcy filing by the OneStop vendor, Enovational, and DNR's assertion of the availability of commercial-of-the-shelf (COTS) and/or software-as-a-service (SaaS) solutions in the marketplace which can be procured through the RFP process. As a new solution will be selected via the RFP process, which is still in process, current cost or schedule estimates are not available at this time.

- *To what extent did this cause any deterioration of services?*

  During the period beginning in March of 2022, when Enovational filed for Chapter 11 bankruptcy, through the finalization of the asset sale to Ernst and Young, LLP (E&Y) effective October 2022, DoIT put a hold on all new OneStop portal work. Although no new work was being initiated, Enovational continued to provide maintenance and operations support as needed and the portal did not experience any outages or service interruptions during this time. New work has resumed on the portal following the successful transition to E&Y.

- *What are the cybersecurity risks? Is OneStop getting necessary upgrades and bug fixes?*

  With the finalization of the asset sale by E&Y in October 2022, the hosting of the OneStop portals production and user acceptance testing (UAT) environments was transitioned to DoIT's managed Amazon Web Services (AWS) instance. DoIT has engaged with E&Y and DoIT security consultants to perform a full Authorization to Operate (ATO) in order to ensure the system is adequately hardened against security vulnerabilities. In parallel with the ATO, DoIT and E&Y are working to identify emerging security vulnerabilities or gaps that require immediate updates or system enhancements.

- *What other OneStop applications are supported by this vendor?*

  The OneStop portal provides access to approximately 350 applications/forms across 13 state agencies. Approximately 80 of these forms/applications, along with associated workflows, have been automated.

- *Are there proprietary applications that will be difficult or expensive to maintain?*

  The formability platform, which is the underlying technology that powers the OneStop portal, is now owned by E&Y. E&Y, under the OneStop Agile Automation Services Task Order Request for Proposal (TORFP), provides formability platform maintenance and enhancements at no cost to the state. The state pays for the maintenance of Maryland's forms and applications that have been deployed on the OneStop portal and state specific platform enhancements.

- *What is the long-term solution? Will Ernst and Young keep this service or will this be sold when a buyer is found?*

  E&Y acquired the formability platform, which is the underlying technology that powers the OneStop portal, with the intent to continue to support the state of Maryland and expand into other states. E&Y is not seeking to sell the formability platform.

- *What plans does DoIT have to manage this kind of vendor risk with modules supported by other vendors?*

  DoIT will be evaluating all platforms that have a heavy reliance on vendor support for business continuity and ensuring there are dedicated resources to support these platforms internally.

Operating Budget Recommended Actions

1. **Reduce general funds for Maryland AIDS Drug Assistance Program major information technology project and authorize special funds.**

   DoIT concurs with this recommendation.

2. **Delete funds for the Department of General Services' AS400 replacement system major information technology project.**

   DoIT concurs with this recommendation.

3. **Adopt narrative requesting a report on Managing for Results goals and indicators for services to State agencies.**

   DoIT concurs with this recommendation.