Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

Department of Information Technology
Fiscal Year 2023 Operating Budget
Response to Department of Legislative Services Analysis

Senate Budget and Taxation Committee

Education, Business and Administration Subcommittee

The Honorable Nancy J. King, Chair

March 3, 2022

House Appropriations Committee

Public Safety and Administration Subcommittee

The Honorable Tony Bridges, Chair

March 7, 2022

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 evolving cybersecurity threats and solutions the State faces. The following testimony addresses the requests for comments in the analysis, as well as the DLS recommendations.

Issues

1. **Cybersecutity Threats and Solutions are Evolving: What Should the State do to Keep Up?**

   The department should be prepared to brief the committees on its efforts to update cybersecurity processes that have become more difficult to implement during the pandemic.

   Since the passing of the Maryland Cyber Defense Initiative executive order in June 2019 the Office of Security Management (OSM), led by the State Chief Information Security Officer (SCISO), has made significant progress in securing the cybersecurity posture of the State. Although the State faced many challenges during fiscal 2020 and 2021 due to the pandemic, OSM managed to transformationally change the security program. The following includes a non-exhaustive list of OSMs efforts to date.

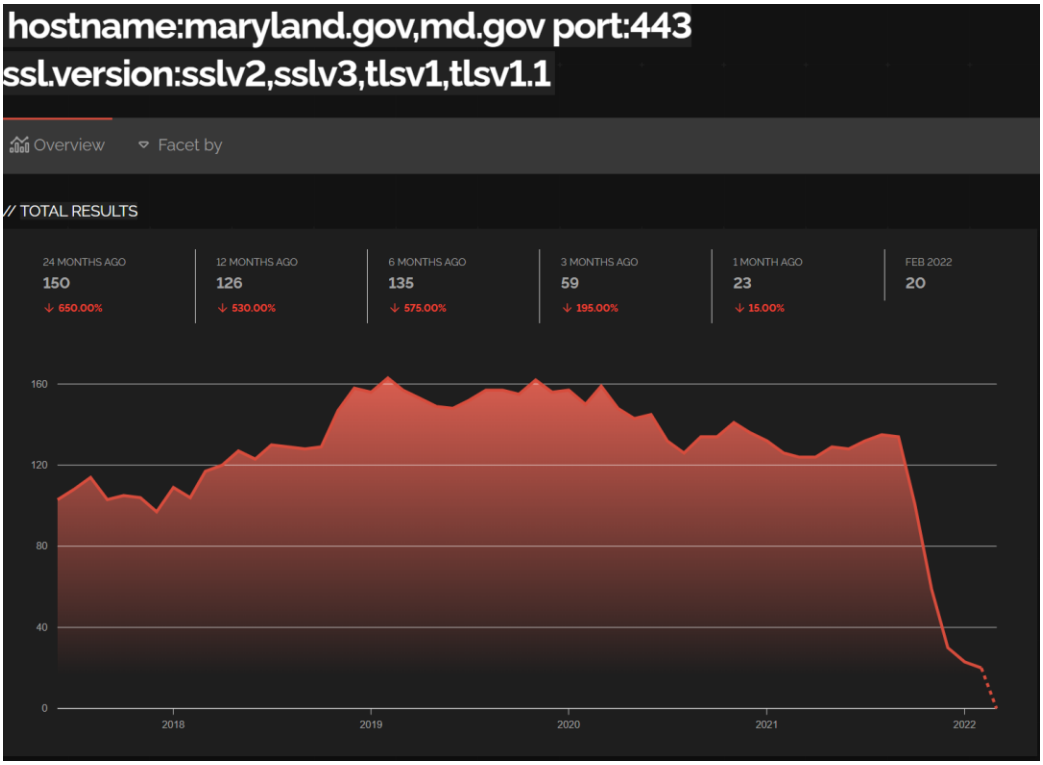
   - Security Operations
     - Transition from a outsourced Security Operations Center (SOC) to an in-house 24x7x365 SOC;
     - Updated the email system to better filter malware and phishing emails;
     - Implemented network-based volumetric Denial of Service and Distributed Denial of Service protection; and
     - Implemented takedown service for State-government impersonation sites, including those used to perpetrate unemployment insurance (UI) fraud.
   - Vulnerability and Risk Management
     - Improved network-based risk assessments for assets on networkMaryland;
       - Direct remediation action on externally identifiable high-risk items (RDP, Unsupported encryption, etc).
     - Tripled the size of the vulnerability management program (almost 30,000 assets in the system); and
     - Transitioned the vulnerability management process into ServiceNow, our Information Technology Service Management (ITSM) platform.
   - Workforce Development
     - Created new cybersecurity job classifications based on the National Institute of Standards and Technology (NIST) SP-800-181 to align with the National Initiative for Cybersecurity Education (NICE) framework. By using this framework, OSM is able to develop, attract, and retain qualified cybersecurity professionals.
   - Threat Intelligence and Information Sharing

- Established automated indicator sharing with MS-ISAC, Oklahoma, and Texas, allowing for near real-time blocking of threats detected by other States and partners; and
- Imported vulnerability intelligence into ServiceNow, allowing us to track and prioritize vulnerability remediation efforts.

■ ServiceNow Security Operations and Governance, Risk Management and Compliance (GRC)

- Implemented several security automation and standardization tools, including the GRC module which allows OSM to centrally manage and track our annual audits and reviews of firewall configurations with agencies; and
- Automated data collection around security events.

Another important item of note is the actions and results we are taking to improve our managing for results (MFR) metrics. To improve security and metrics, OSM engages in periodic meetings that include these metrics. As a result, we have seen dramatic improvements in these areas, such as websites running unsupported encryption protocols (fewer represents an improvement as shown below).



2. **DoIT Surveys State Agencies about Cybersecurity Risk Mitigation Practices**

DoIT should be prepared to brief the committees on progress made in replacing legacy systems.

As the analysis from the DLS acknowledges, the fiscal 2023 budget includes $115 million in general funds that have been allocated to the Major Information Technology Development Project Fund (MITDPF) for 32 projects. This is the highest amount of general funds and projects receiving general funds to date, as the increase in the MITDPF has grown from approximately $20 million in 2014 to $115 million in 2023. It is anticipated that this will continue to increase to $116 million in fiscal 2024.

The total number of projects funded, including active projects funded in prior years and projects that do not receive general funds, is 53. Of those projects, 95% of them consist of modernizing existing systems and processes. There are a number of factors that are taken into account when recommending the replacement of legacy systems, all of which are directly tied to security assessments, surveys and automated discovery tool sets managed by OSM. These factors, among others, are taken into account when DoIT compiles the recommended major IT projects for funding in the upcoming year.

3. **MDH Ransomware Attack**

DoIT should be prepared to brief the committees on the status of the MDH ransomware attack, coordination between departments in response to the incident, lessons learned from the attack, and new policies and practices contemplated or adopted in response to the attack.

It is important to note that the MDH ransomware attack is still an active criminal investigation. For that reason, there are still many details that DoIT cannot share.

Regarding the overall incident response status, the incident response team used the framework described by NIST SP 800-61R2. This framework describes a standard flow progressing from detection to containment, to eradication, and recovery.

As previously described, MDH identified the incident and analyzed the information available at that time to recognize the severity of the incident. At the direction of the SCISO, MDH initiated containment action by isolating each of its network locations from the backbone network. The response activities to date have involved close coordination between MDH, DoIT, MCAC, and MDEM.

In the weeks since then, the response resources have been focused on prioritized eradication and recovery of critical systems. This is a complex process that involves using an amalgamation of specialized tools and highly trained personnel to clear system components and data to bring the business function back online. In many cases, where system components were either no longer supported or nearing end-of-support, modernization efforts were expedited.

There is also a parallel effort to restore user workstations that is combining planned hardware refresh activities with traditional restoration activities to better support full service recovery for MDH.

As the investigation concludes and recovery activities continue, there are many takeaways from the event. It is important to note that it would be irresponsible to share lessons learned that characterize system weaknesses, especially if not fully resolved. There are several items that can be publicly shared and would be of broad value to many organizations beyond MDH and the State. Many of these needs were anticipated and already underway.

Improvements Already Underway

1. Ensure that business continuity plans consider the potential for a cyber-disruption or a general unavailability of technology resources. This includes validating that agencies fully understand the difference between disaster recovery (DR) and business continuity planning (BCP) and how to apply each of those to sustain operations.

   In 2021, as part of the changes codified in the 2020 legislative session, MDEM developed new guidance for agencies that included cyber disruptions as part of the all-hazards approach to planning. This guidance now includes language for recovery time objectives and recovery point objectives as part of that planning.

2. Activation of the State Cybersecurity Incident Response Plan did not follow expected paths. Engage in tabletop exercises to identify gaps in clarity of incident response plans to ensure consistent response.

   While the activation of the plan occurred quickly, it relied on phone calls between individuals rather than to the State Security Operations Center. Engaging in proactive training exercises, such as table top simulations, will aid in reliable incident response. This activity, at the State level, was

in its initiation phases as part of preparation and planning coordination between DoIT and MDEM before the incident.

Sustains

1. The cybersecurity incident response plan facilitated timely containment of the incident.
2. Roles and authorities were clear throughout the incident response.
3. Internal communications functions performed well in keeping employees apprised of the current status of recovery efforts.

Opportunities for Improvement

1. The State Cybersecurity Incident Response Plan did not have after-hours contact information for the insurance carrier liaisons at the State Treasurer's Office.

   This issue has been resolved.

Operating Budget Recommended Actions

1. **Adopt narrative requiring the Department of Information Technology's Managing for Results goals and indicators to include value and costs, instead of limiting to workload and efficiency measures.**

   DoIT concurs with this recommendation.

2. **Adopt narrative requiring the Department of Information Technology to report on spending funds in the Dedicated Purpose Account to support cybersecurity efforts.**

   DoIT concurs with this recommendation.

3. **Adopt narrative requiring the Department of Information Technology to submit an update on the Remote Workforce Enablement Major Information Technology Development Project.**

   DoIT concurs with this recommendation.

4. **Adopt narrative that requires the Department of Information Technology to report on spending and planning regarding the federal Infrastructure Investment and Jobs Act.**

   DoIT concurs with this recommendation.

5. **Adopt narrative requiring the Department of Information Technology to review and update standard pricing schedules for over-the-air television and radio resource sharing agreements.**

   DoIT concurs with this recommendation.

6. **Adopt narrative requiring a report on the positions of the State Chief Data Officer and State Chief Privacy Officer.**

   DoIT concurs with this recommendation.