LARRY HOGAN
Governor
BOYD K. RUTHERFORD
Lieutenant Governor

MICHAEL G. LEAHY
Secretary
LANCE SCHINE
Deputy Secretary

FISCAL YEAR 2020 BUDGET HEARING

Testimony of
Michael G. Leahy, Secretary

Senate Budget and Taxation Committee
February 26, 2019

House Appropriations Committee
February 27, 2019

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 budget.

The DLS Analysis focuses on three key observations, which include the transition to a fee-for-service model for enterprise IT services, the status of the cybersecurity program, and DoIT's above average vacancy rate. The following testimony addresses the requests for comments in the analysis as well as the DLS recommendations.

Requests for Comment

1. **Cybersecurity**

   - **The department should be prepared to brief the budget committees on steps taken to ensure that there is continuous cybersecurity training.**

     DoIT understands the importance of a cybersecurity awareness program as a part of the overall defense against one of the most prevalent cybersecurity threats: social engineering. In fiscal 2018 it was determined that the cybersecurity training solution, based on vulnerable Adobe Flash technology, needed to be replaced. A Request for Proposal (RFP) was released for its replacement, which took longer than anticipated. There is a contract currently in place, and a plan has been developed by our new Chief Information Security Officer (CISO) to make sure that the program is adequately staffed moving forward. Additionally, a sustainable chargeback model is in place in order to provide uninterrupted security awareness training to any State agency.

100 Community PL Crownsville, MD 21032-2022
Tel:(410)697-9700 TTY Users: Call via Maryland Relay

2. **Oversight of Major IT Projects**

    - **DLS recommends that the budget committees adopt committee narrative requiring DoIT to develop Agile-specific MFR indicators for the fiscal 2021 budget.**

      DoIT agrees with this recommendation.

Issues

1. **Enterprise IT Services**

    - **The department should be prepared to brief the committees on efforts to provide high-quality services and measure service quality.**

      DoIT has focused its efforts around the underlying processes, which target engaging the correct resources quickly and accurately, providing support resources with tools to effectively manage tickets, and assessing the customer's level of satisfaction with the support provided. While the centralization of IT and IT staff may have resulted in the introduction of processes which are different from those previously employed, these processes are designed to improve efficiency and effectiveness of service delivery. As noted in the DLS Analysis, DoIT has been focused on measuring workload in part to locate resources where they are needed most. Tools have been introduced which have increased the number of service requests resolved on first contact. Bi-weekly meetings are held to discuss team performance and customer satisfaction, identify areas of improvement, and plan for initiatives which may be critical to that support team's customers.

      In regards to hardware and software upgrades, one of the major concerns expressed was the impact of software patching on agency bandwidth. To address this issue DoIT has deployed a new system for patching end user devices - Tanium. Unlike the previous system which required every device be patched from a centrally located server, Tanium patches one device within an environment and then uses the patched device to provide the deployed patch to other devices within that environment. Tanium also allows greater flexibility in terms of scheduling so that patches are deployed more quickly and in line with agency specific requests. The result is significantly less impact on agency bandwidth and end user devices which are secure and up-to-date in regards to critical operating system patches and anti-virus definitions. Today, 99.94% of end user devices have received critical OS patches, 96.65% of servers are critically patched, and 98% of all devices have the most current virus definitions installed.

- **The department should be prepared to brief the committees on how it ensures that agencies' priorities are managed.**

  As mentioned in DLS's analysis, DoIT will fully transition to a cost allocation model (referred to by DBM as a "fee-for-service model") for enterprise IT services in fiscal 2020. In collaboration with DBM, a financial schedule for the services DoIT provides has been developed, which will allow the agencies to be aware of the costs before the start of the fiscal year. DoIT will be implementing the Technology Business Management (TBM) Model that will provide the agencies with a full transparency of the costs associated with each service they are being provided. It is designed to provide a shared decision-making model for technology and business leaders. By implementing TBM as the basis for the shared services model DoIT will be able to manage the cost, consumption and performance of services offered by DoIT, provide better transparency, and ensure accountability at multiple levels of government.

  The Department has also been in collaboration with the Office of Management and Budget (OMB) to ensure implementation of TBM. OMB has a mature practice based upon the TBM model, and DoIT intends to leverage OMB's experience and knowledge gained to accelerate implementation.

  DoIT has created a Shared Service Catalog (SSC) that includes all of the IT service offerings provided by security, applications systems management and infrastructure. The agencies are able to view the SSC on DoIT's website to determine the services required. DoIT has also established a standard Memorandum of Understanding (MOU) for each agency in the Enterprise, which will layout the responsibilities and expectations of each agency. An appendix to this MOU will be the services selected by the agency.

  Part of the organizational restructure that DoIT is undergoing, is the creation of Portfolio Officer (PO). The PO's will directly interact with the agencies, as well as provide them with a full transparency of the services being provided to include the costs associated with each level of service. They will be responsible for negotiating the MOU's with the agencies, ensuring service delivery, and monitoring the overall quality of the services being provided by DoIT.

2. Cybersecurity

- **The department should be prepared to brief the committees on its efforts to minimize the risks of social engineering.**

  In order to reduce the risk of social engineering, DoIT is taking a multi-pronged approach. Though security awareness training is a vital component of a security program in order to reduce the risk of an employee falling for a social

engineering campaign, there is a technology component that must be addressed as well. It is important to note that sources have shown security awareness training alone to be an ineffective method to thwart social engineering, including phishing campaigns. According to the Verizon 2016 Data Breach Investigations Report, 30% of employees can be expected to open a well-crafted malicious email, and 12% to click a malicious link or attachment, even among organizations receiving security awareness training. These numbers show that DoIT cannot rely solely on security awareness training to combat the threat of social engineering.

A social engineering campaign cannot be successful if would be attackers are thwarted earlier in the kill chain, before they can make contact with a State employee. Phishing is one of the most common types of social engineering and is a good example of this principle. DoIT is looking at ways to enhance the State's email filters in an effort to reduce the chance that malicious emails even make it to an employee.

DoIT intends to conduct a security assessment of the State security practices which will include an assessment of our email filters and their ability to catch malicious emails before ever making it to a State employee. DoIT will hire a security "red team" made up of white hat hackers to attempt to circumvent our email filters. The result of this endeavor will be recommendations on how the State email systems can be better hardened against social engineering campaigns. This is a process that will allow DoIT to better address future phishing and social engineering campaigns. This endeavor also aligns with the Verizon 2016 Data Breach Investigations Report top recommendation for thwarting social engineering campaigns.

- **DLS recommends that the State cybersecurity positions be considered in the Annual Salary Review (ASR) process in the fiscal 2021 budget cycle.**

DoIT concurs with this recommendation. The State has not been able to attract enough top talented individuals in the field of cybersecurity due to offering much lower salaries than private sector or even other public sector entities.

3. Personnel

- **The department should be prepared to brief the budget committees on the high vacancy rate and difficulties in retaining personnel. This should include any actions being taken to recruit senior level management.**

Nationally, IT professionals are in high demand and in short supply. Many agencies experience difficulty in attracting and retaining minimally viable candidates to state government IT positions. The primary cause is that salaries offered by the State are below what other employers in the area are able to offer. The private industry, federal government, as well as counties and local

municipalities all offer more in the way of compensation.

In an effort to manage to these difficulties and reduce the high turnover rate, DoIT has been working with DBM's Compensation and Classification division to get positions reclassified at competitive rates. The revised organization chart is a high level snapshot of the pending reorganization within DoIT, in an effort to increase efficiencies across the organization and attract senior level management. There are several divisions that are in the development stages, such as Application Development, Innovations, and the Data Office.

Recommendations

1. **Delete funds for the Statewide Grant System. This is a new initiative to develop a statewide system for tracking grants. According to the Information Technology Project Request, initial functions such as developing a project charter and project management plan are not scheduled to be completed until fiscal 2020. In spite of this late start, the project has an aggressive schedule to complete a Request for Proposals by the end of calendar 2019 and have a vendor on board at the end of the fiscal year. Since procurement is late in the year and short delays can move the procurement into fiscal 2021, it is recommended that the funds be deleted and instead appropriated in fiscal 2021.**

   In fiscal 2017, the State of Maryland expended $14.4 billion in Federal funding, an increase of 6% from $13.5 billion in fiscal 2016. Federal funding is sometimes passed through to subrecipient government agencies, or nonprofits. In fiscal 2017, the State of Maryland granted $467,328,699 to subrecipients, an increase of 22% from $384,100,405 in fiscal 2016 (State of Maryland Single Audits, SB and Company, LLC). The increases in Federal funding and pass through funding to sub-agreements reflect growth and opportunity for Maryland communities.

   The acceptance of a Federal award is accompanied by mandatory obligations to fulfill programmatic and fiscal reporting requirements. As such, the State is required to demonstrate compliance with Federal statutes, regulations and terms and conditions of its Federal awards. All recipients and subrecipients of Federal funding must demonstrate compliance with the Uniform Guidance, Title 2 Code of Federal Regulations, Part 200, Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards.

   Monitoring compliance with the Uniform Guidance is challenging for the state because there is no statewide grants management system. For over three years, the Governor's Grants Office (GGO) has collaborated with DBM and DoIT to systemize Federal funding compliance, reporting, and grants management best practices. The GGO has reviewed data from a survey of state grant managers, interviewed state grants points of contact and key individuals, analyzed Maryland's Single Audit findings, and explored grants management solutions adopted in other states. By standardizing and streamlining grants

management, Maryland will:

- *Align State grant management practices with the Federal Uniform Guidance requirements*
- *Centralize oversight, coordination and compliance of grants throughout the grant lifecycle, statewide*
- *Eliminate duplicative, antiquated, labor intensive, time consuming manual systems in state agencies*
- *Create accessibility and transparency of grants management to the public*
- *Automate grant research and grant notifications to align to the State's strategic goals*
- *Integrate the State's financial management system, grant budgets and cost allocation methodologies*
- *Improve grant forecasting and expand the portfolio of grant revenue sources*
- *Increase the quality of new and recurring proposals through an archive of data and grant documents*
- *Professionalize grants management staff by increasing the prevalence of on-demand training and technical assistance in nationally accepted best practices and the Uniform Guidance*
- *Decrease new audit findings and improve the ratio of new findings to $Billions of Federal funding managed*
- *Increase accountability and decrease risk by improving the management of grant subrecipients*
- *Automate grant awards and decrease the time period between grant award and spending*
- *Maximize Indirect Cost recovery*

It is essential that the $2,000,000 for this system be funded, so GGO can with immediacy proceed with their plan to maximize federal funds.

2. **Adopt the following narrative:**

   Managing for Results Indicators for Major Information Technology Projects Developed Using Agile: For major information technology (IT) development projects, the Department of Information Technology (DoIT) has transitioned from the Waterfall method to the Agile method. Some of the key Managing for Results (MFR) performance indicators measure rebaselining, which is more suited for Waterfall and less helpful with Agile. DoIT should develop performance indicators more suited to the Agile approach. This can include indicators measuring on-time delivery, product quality, business values, and project visibility. The indicators should be included in the Governor's fiscal 2021 Budget Books.

   DoIT agrees with this recommendation.