



Department of Information
Technology
Fiscal Year 2018 Operating Budget

TESTIMONY OF

Luis Estrada, Deputy Secretary

Senate Budget and Taxation Committee

The Honorable Edward J. Kasemeyer, Chair

February 7, 2017

House Appropriations Committee

Subcommittee on Public Safety and Administration

The Honorable Keith E. Haynes, Chair

February 8, 2017



Testimony

Good afternoon, Mr. Chairman and members of the committee. I am Luis Estrada, Deputy Secretary of the Maryland Department of Information Technology. I am joined by Albert Bullock, Assistant Secretary and James Appel, Executive Financial Officer. Thank you for giving us the opportunity to provide this testimony, and thank you Patrick for all the hard work you put into creating this analysis.

Over the last year, we have expanded our Enterprise organization to fulfill the core IT service needs of 33 small and mid-sized agencies and offices. This Enterprise IT effort began in July 2015. By November 2016, we migrated the small-to-mid sized cabinet agencies and offices into the Enterprise. We now support over 12,000 users in the State while maintaining a 90+% customer satisfaction rating for our Service Desk each month. We have lifted agencies to a common baseline with respect to capabilities, security, and quality. Our efforts to improve the baselines in service delivery and cybersecurity for all enterprise agencies will continue in the coming year. We are also actively aligning our IT service delivery organization to the industry standard IT Infrastructure Library, or ITIL, with an eye towards improving both the quality and consistency of the services we deliver at the Department.

We recognize cybersecurity as a priority. We are improving the posture of agencies across the executive branch, and more directly improving those within the enterprise. Our written testimony goes into greater depth about how DoIT is working to improve the cybersecurity posture of the State.

With respect to the Major Information Technology Development Project Fund, we recognize that the number of out of cycle project requests has increased. To improve forward planning, DoIT is initiating an Enterprise Solutions Planning Initiative (ESPI). This IT project request (ITPR) will allow for central planning of needs identified from multiple agencies earlier, and allow us to take an enterprise-wide view of the State's needs. We believe this will reduce the number of ITPRs submitted as out of cycle requests. We oppose the recommendation to reduce our oversight funding by \$1,000,000 as this will be detrimental to the progress of the program. First and foremost, we cannot predict a year in advance which projects will be in need of additional oversight support. Secondly, as the State transitions to an agile Software Development Lifecycle, agencies will need additional support and guidance from DoIT to assist in this transition. Furthermore, with several major projects currently completing the procurement phase, more projects will enter the implementation phase in FY18, which requires a greater degree of oversight support.

The State's agile System Development Life Cycle (SDLC) is a framework intended to reduce the risk of project failure through the application of incremental and iterative solution delivery. This approach focuses on the benefits of the agile method to improve the delivery of information technology projects. Aligning our work with the Governor's priorities and agency missions, breaking work down into loosely-coupled components or services, and delivering iteratively in rapid learning cycles, delivers more value in less time and saves many millions of taxpayer dollars. A lean-agile approach forces delivery of value more frequently, allowing us to detect small failures early and treat them as learning

opportunities leading to an improved product. This industry-proven technique is superior to the prior “waterfall” approach, and will help the State improve its digital government services.

We also ask that the funding for the Shared Human Services Project (MD Think) not be restricted to the federal funds as the federal Advanced Planning Document was approved on February 2nd.

As the Department changes with the Enterprise plan, and as we implement the ITIL framework, we will update and refine our Managing for Results (MfR) measures. Establishing service delivery quality metrics is a key part of the ITIL framework, and as we continue to document our service definitions and internal processes, more applicable MfRs will be created.

We would like to address our future budgeting plans for IT across the state. As we finalize the enterprise service catalog, we will track the actual costs for providing these services, and provide each agency with a detailed accounting of services delivered. Additionally, we will participate in each agency’s budget planning for FY19 to include a clear forecast for IT service costs.

Finally, we recognize the difficulties faced in competing for IT talent with surrounding federal and private sector entities. We will work with the Department of Budget and Management to explore options to increase retention and reduce vacancies. With that said, we would ask that the turnover rate not be increased as we intend to fill most of our vacancies in Fiscal Year 2018, if not before.

Additional, more specific information pertaining to Cybersecurity, the Enterprise, and our plans for the MITDP are found in our written testimony and I urge you to review it at your leisure.

On behalf of Governor Hogan I thank you for your time today. I am happy to answer any questions that you may have.

Issues

DLS

Cybersecurity: The department has published cybersecurity performance measures. The agency will provide vulnerability assessments, penetration tests, or audits to 20 agencies each fiscal year. A cybersecurity awareness program has also been implemented and 90% of employees are participating. DoIT advises that the number of staff trained is limited by the number of licenses and that purchasing additional licenses could increase this indicator beyond 90%. **DoIT should be prepared to brief the committees on the costs and benefits associated with purchasing additional licenses.**

Cybersecurity: In recent years, DoIT has provided more resources for cybersecurity. There are signs of improvement, but audit findings continue to show weaknesses. **In spite of all the training, increased resources, and improved policies, audits still reveal critical security weaknesses. The department should brief the committees on how it plans to address these weaknesses.**

DoIT

Employees must be trained and consistently reminded about information security. The DoIT Security Training program has enrolled 41,555 State employees and has achieved a 93% participation rate. The remaining approximately 8,400 State employees not covered by DoIT's security training program either receive security training by other means, or are not in job classifications that require it. We feel the current level of licenses is appropriate, and rather than increasing licenses, we will work with local managers to increase the participation rate of existing users.

DoIT provides agency penetration testing and vulnerability analysis as a service upon request. The ongoing audit program ceased in 2016 as we evolved our cybersecurity strategy. As agency heads determine and resource their security requirements, DoIT will revise our cybersecurity metrics.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) expects that the majority of cyber incidents affecting state, local, tribal, and territorial (SLTT) governments will continue to be opportunistic in nature. They also believe the sophistication of routine malware, cyber threat actors, and their tactics, techniques, and procedures (TTPs) will continue to increase. DoIT is addressing these weaknesses by migrating agencies to the Enterprise, and then iteratively improving their security posture. Migration to the Enterprise has two trains; the deployment of standards (policies, applications, and tools), and alignment of each agency's infrastructure into a secure Enterprise Architecture. This is a long term initiative as decades of technologies and applications are absorbed into security oversight for the first time.

Initially, DoIT assumes management of an agency's endpoint and perimeter defenses, and then establishes a monitoring program to ensure the equipment and the personnel are in fact working within an identified security profile. Today, all of the agencies in the first two phases of the Enterprise IT project are now running on next-generation firewalls, an improvement over their legacy systems.

This provided the benefits of Intrusion Detection and Prevention capabilities, enhanced traffic analysis, and centralized logging. These logs are now being analyzed by DoIT's 24x7x365 Security Operations Center. A baseline firewall ruleset has been developed which improves upon the rulesets currently deployed. The first version of the baseline is in the process of being deployed to all agencies in the Enterprise. The baseline ruleset will then be iteratively improved over time. This provides a standard level of increasing security at the boundary of the agencies' networks.

Similar processes are taking place for protecting end-user devices (computers, tablets, phones). Standard security software is being deployed to each group of devices, and centralized management of these devices is being established. This allows DoIT to ensure that each device has the latest versions of software and that critical vulnerabilities are remediated in a timely fashion through a centralized management platform. DoIT has also deployed change management practices, which adds a layer of security through better operational control of systems.

Finally, DoIT has adopted the NIST Cybersecurity Framework, and has promulgated those policies throughout the executive branch.

DLS

DoIT planned to have one multi-agency security drill in fiscal 2015 and three in fiscal 2016. The Maryland Emergency Management Agency (MEMA) and the Air National Guard work with DoIT to develop drills that test responses to cybersecurity threats that impact State IT systems. There were no drills in fiscal 2015 or 2016. **The department should be prepared to brief the committees on the lack of multi-agency drills and exercises. DoIT should also discuss how it will increase the number of drills and exercises in fiscal 2017 and 2018.**

DoIT

Multi-agency drills require a great deal of manpower and coordination to become a valuable use of training time. In 2016 however, DoIT, in conjunction with MEMA, conducted a cyber exercise that involved every agency to include the National Guard, as well as several Federal partners. DoIT, along with the National Guard, participated in the 2016 Cyber Guard series of exercises sponsored by US CYBERCOM. In 2016, we also participated in an USCYBERCOM Cyber Law and Policy exercise, and two Federal Emergency Management Agency Region 3 exercises with our regional partners. We are participating in the Cyber Guard series again this year (ongoing), the Law and Policy exercise again later this month, and in a FEMA region 3 cyber exercise this June.

DLS

The department should be prepared to brief the committee on its role in the Maryland Cybersecurity Council.

DoIT

Former Secretary Garcia chaired the Current Operations and Incident Response subcommittee, and briefed the committee on 3 tasks and objectives:

1. Identify tools and methods used to prevent cyber incidents and respond to cyber incidents
2. Identify tools and methods used by the State of Maryland and compare/contrast them with other leading states
3. Deliver a comprehensive statewide cyber incident response plan. The plan is in final execution phase and as mentioned prior, has been exercised within the State Emergency Management construct. Of note, this plan is one of a handful of state cyber disruption plans that is fully coordinated with State and Federal Emergency Response Plans, and thus is already in compliance or complementary to the National Cyber Incident Response Plan released by DHS in January.

MITDP Items

DLS

To keep the legislature informed about the status of major IT projects, DoIT has notified DLS as project planning begins or when projects move from planning to implementation when the legislature is not in session. These are referred to as out-of-cycle ITPRs. In the recent interim, there has been a spike in the number of out-of-cycle ITPRs. As DoIT moves to the Agile approach to major IT project development, this process may become obsolete and another process may need to be developed. **It is recommended that DLS and DoIT work together to develop a process for keeping the legislature informed about changes in major IT projects when the legislature is not in session.**

DoIT

DoIT has worked with our analyst Patrick Frank to develop new reporting criteria and methodology to account for our transition to lean agile development. This has included briefing Patrick and roughly 25 other members of the DLS office on the new approach, and will continue to keep DLS informed of any future metrics and process changes. As agile adoption increases, we will work with DLS to develop a process for keeping the legislature informed about changes in major IT projects along with the standard Midyear and End of Year Reports.

In addition, the Enterprise Solutions Planning Initiative (ESPI) ITPR has been established to plan fewer, less duplicative, and broader initiatives which will supplement the many planning and out of cycle ITPRs submitted in the past. This will provide support for earlier identification of agencies needs and a significant decrease in the amount of planning ITPRs that need to be reviewed or out of cycles submitted.

DLS

DHR Shared Human Services Platform - Initial funding (totaling \$13.9 million) was provided in a fiscal 2017 supplemental budget item in March 2016. These funds were restricted pending federal approval.

Risks include interdependencies, organizational culture, and the large scope of this project. Federal funds totaling \$65.2 million (for fiscal 2017 and 2018) are in the DHR budget. **DLS recommends that the General Assembly again adopt language restricting funds pending federal approval.**

DoIT

Given that the Federal Government has approved the Advanced Planning Document for the project, there should be no restriction of project funds to the MITDP.

General

DLS

DLS recommends that DoIT, in cooperation with the Department of Budget and Management's Office of Personnel Services and Benefits, examine the State's IT professionals compensation and compare it with the compensation offered by nearby federal, local, and private organizations. This should include an analysis of nonwage benefits. The departments should also consider partnering with higher education institutions to develop training programs for students to prepare them to be IT professionals that work for State agencies.

DoIT

A report shows that the State's compensation of IT professionals is less than the industry average. This has led to higher employee turnover, higher agency vacancies, difficulty filling key positions, and the use of contractors in key positions. DoIT acknowledges difficulty in competing with federal and private sector entities for talent given the State's standard pay scale. DoIT can assist the Department of Budget and Management in examining the issues of recruitment, retention, and compensation of IT professionals. Currently, DoIT is increasing its recruitment efforts with a plan to work with higher education institutions, use social media platforms, and explore other methods.

DLS

Enterprise Tech Support Initiative: The department should be prepared to brief the budget committees on its initiative to expand the support services that it is offering to State agencies.

DoIT

DoIT began migrating day-to-day IT operations in fiscal 2016. Currently, approximately 12,000 State employees are served by DoIT. The process of establishing the Enterprise IT operations teams within DoIT is proceeding successfully. The initial steps in the process involve taking an inventory of all systems and applications, and then preparing DoIT and the agency for integration into the common support model. Agency systems are configured to meet a minimum baseline standard, and then DoIT assumes operational responsibility for the commodity IT services that are delivered to the agency. At the same time, personnel at the agency that previously supported these commodity IT services are transferred to DoIT. At this time two main tracks of work take place.

First, the services delivered to the agency are aligned with the Enterprise standards. This includes security, end user computing, network, and server standards. This allows the baseline security of the agency's IT systems to be elevated and in line with statewide policy and industry best practices. It also allows a more efficient service delivery model, one where service level objectives can be established and service delivery can be measured. Once all of the systems have been remediated and brought to the Enterprise standards, the agency's infrastructure is moved into the established Enterprise Architecture.

Simultaneously, DoIT management meets with all of the new employees to align individual skills and career goals. Since the Enterprise IT agency has a larger footprint there are more employee opportunities. Employees have the potential to specialize in a specific technology or select a different work location when opportunities arise. This has improved the morale among the technical teams and allowed employees to pursue new interests without leaving the State system, improving employee retention.

Equally important is the alignment of DoIT's IT Service Management (ITSM) to the ITIL framework. This is a mature industry standard methodology for delivering IT services. A cornerstone of this alignment is the establishment of a Service Catalog. The DoIT service catalog (<http://doit.maryland.gov/support/Pages/Service-Catalog.aspx>) identifies all of the services delivered by DoIT, their service level objectives, how to order the service, and how to receive help with the service delivery. Each of the services will be supported by detailed design documents (Service Design Package) that outlines all of the configuration requirements and the interdependencies of services, as well as the staffing and technical requirements needed to deliver these services. This increases the maturity level of the IT service delivery to the Enterprise. Along with defining the services in the Service Catalog, a service owner is identified for each service. One person becomes responsible for the maintenance and delivery of each service, and the technical teams are aligned to support each service. These ITIL constructs remove the risk of only one person knowing how a specific service or implementation works, and provides depth of knowledge within teams. It also establishes ownership and accountability to providing services that meet established Service Level Objectives and provides value to the customers.

Finally, DoIT has initiated the assembly of a Service Management Team. The goal of the Service Management Team is to oversee proper execution of the services delivered by DoIT to other State Agencies, and ensure that these services consistently meet and exceed the Service Level Objectives (SLO) set by DoIT and the customer's needs. The members of the Service Management Team will be the primary DoIT point of contact for customers. The Service Management Team's primary customer interface is the Deputy CIO assigned to the customer Agency. The team has met with two agencies this year (Aging and DLLR), and is scheduling additional meetings with all of the agencies to review each respective agency's 2016 IT Service Delivery Report (detailed in the following item).

DLS

State Agency Support Indicators Should Change as Department Reorganizes: The department also supports systems used by State agencies, such as telecommunications systems, wireless networks, a data network, and statewide financial and personnel systems. Surveys suggest that the service provided is perceived to be satisfactory. No surveys have been taken in the last year. DoIT has implemented new software that asks individuals to rate their satisfaction after a service has been provided. As discussed in the Issues section of this analysis, the department is implementing its enterprise tech support initiative. The Department of Legislative Services' (DLS) concern is that these indicators are out-of-date. DoIT should develop new indicators that reflect its new workload.

DoIT

One of the key metrics DoIT uses to measure the quality of the Enterprise support is a survey delivered to all employees who enter a request through the service desk. These surveys, a current MFR, are sent after the service request has been resolved. In 2016 1,850 surveys rating the technician who provided service to the customer were submitted, and 94% of these surveys rated the technician "excellent" or "satisfactory". In this same time period 1,782 surveys rating the DoIT service desk performance were submitted, with 91% identifying a level of performance as "excellent" or "satisfactory".

Additionally, DoIT prepares a service delivery report for every agency that migrated IT services to DoIT as part of the Enterprise plan. These reports identify the results of the initial inventory, highlights of the remediation and standardization efforts, performance of the DoIT service desk, an analysis of the service desk tickets that DoIT received related to the respective agency, and an analysis of the services DoIT provided to the agency. The reports are delivered to each agency during February and a sample report provided to the Department of Aging is included in this testimony as an appendix.

As service level objectives are defined for each service in the DoIT service catalog, new measurements and reporting of these services will be implemented. DoIT will make these service reports available publically on the DoIT web site.

Recommendations

Recommended Actions

Action	Funds
1. Video Streaming of Legislative Sessions - DLS recommends that the funds be contingent on SB 253/HB 438 which requires that the floor sessions be streamed.	
2. Reduce funding for major information technology project oversight.	\$ 1,000,000
3. Add language to reduce authorization to spend reimbursable funds related to an increase in the turnover rate.	
4. Increase turnover rate to 6%.	315,000
5. Adopt narrative requiring the Departments of Information Technology and Budget and Management to examine information technology personnel compensation.	
6. Adopt narrative requesting a report on the status of the Agile major information technology project development approach.	

Responses to Recommended Actions

- DoIT does not have a comment on this recommendation.
- DoIT opposes this recommendation. First and foremost, we cannot predict a year in advance which projects will be in need of additional oversight support. Secondly, as the State transitions to an agile Software Development Lifecycle, agencies will need additional support and guidance from DoIT to assist in this transition. Furthermore, with several major projects currently completing the procurement phase, more projects will enter the implementation phase in FY18, which requires a greater degree of oversight support.
- DoIT opposes this recommendation. 4 additional PINs have recently been transferred out of the Department, reducing our turnover rate, and we will continue fill the remaining vacancies. The Commission to Modernize State Procurement intends to normalize procurement position classifications, which will help DoIT in filling procurement vacancies.
- DoIT opposes this recommendation - See #3. Increasing the turnover rate creates a disincentive to staff open positions. As we build an Enterprise IT organization, we will depend on these positions to scale the department and deliver quality service. We believe the current rate is more appropriate. Currently, DoIT is increasing its recruitment efforts with a plan to work with higher education institutions, use social media platforms, and explore other methods.
- DoIT supports this recommendation and believes that the Department of Budget and Management, which has Statewide Personnel responsibilities, should be the lead agency on this activity and DoIT will fully support this effort.
- DoIT already reports to the Legislature twice a year on the status of MITDPs in a Midyear and an Annual report. We will include a section in these reports which addresses the agile transition generally, as well as discussing agile transitions specific to each applicable project individually.