State of Maryland
Department of Information Technology

LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

MICHAEL G. LEAHY
Acting Secretary

Department of Information Technology Fiscal Year 2019 Operating Budget

TESTIMONY OF

Michael G. Leahy, Acting Secretary

Senate Budget and Taxation Committee

The Honorable Edward J. Kasemeyer, Chair

March 01, 2018

House Appropriations Committee

Subcommittee on Public Safety and Administration

The Honorable Keith E. Haynes, Chair

February 28, 2018

Department Of
INFORMATION
TECHNOLOGY

Good afternoon Mr. Chairman and members of the committee. I am Mike Leahy, Acting Secretary of the Maryland Department of Information Technology. I am joined by Lance Schine, Deputy Secretary, Assistant Secretary Stan Kizior, and James Appel, Executive Financial Officer. Thank you for giving us the opportunity to provide this testimony to the general assembly. I would also like to thank Patrick Frank, our DLS analyst, for all his hard work. The Department of Information Technology has several major initiatives and I would like to give you a brief overview of them and provide more details in our written testimony. The written testimony also addresses the items mentioned by Patrick in his analysis.

Cybersecurity
The Rural Broadband Project
The "One Stop Portal" modernization project
The Enterprise, which we are now calling "Shared Services"
Data Centers
Revising our Managing for Results and other metrics that will provide better detail and customer service for the State agencies serviced by the Department.

On behalf of Governor Larry Hogan, I thank you for your time and welcome any additional questions from the committee.

1. Cybersecurity

Review of Cybersecurity Standards, Policies, and Procedures: The Department is responsible for developing, maintaining, and enforcing IT policies, procedures, and standards. The Department is also required to provide technical assistance, advice, and recommendations concerning IT matters, which includes cybersecurity. Recent audit findings identified areas in which the State's cybersecurity efforts can be improved. Cybersecurity social engineering concepts also offer guidance for reducing security risks. Concerns are raised about staffing stability. **The Department should brief the committees on its cybersecurity efforts.**

See below

In conclusion, keeping State IT systems secure is critical. This task is complicated by the nature of the threat. Cybersecurity threats are constantly evolving as cyber criminals try to stay one step ahead of the State's efforts to keep data safe. Unfortunately, cybersecurity has no finish line. Cyber threats will keep evolving. As the State neutralizes one threat, another emerges. The key to success is constant vigilance. The best that the State can do is ensure that sufficient resources are available to meet this threat. **The Department should be prepared to brief the committees on its cybersecurity efforts.**

Summary

the Department is continuously enhancing our cybersecurity program by deploying comprehensive and cost-effective processes and technology throughout the Executive Branch. This past year we have made significant improvement to such areas as: Network Security, Data Security, and Endpoint Protection.

Policy

Created 29 policies based on the Risk Management Framework and Security Controls as recommended by the National Institute of Standards and Technology (NIST).

Firewall

- Palo Alto Next Generation Firewall
- Moved 41 agencies to third generation firewalls with advanced features including application awareness, anti-virus and anti-malware, advanced persistent threat detection, zero-day malware detection and protection, and user-based access controls.
- These new firewalls increase the security posture of the state by being able to defend against the threats that are most common today and protect against more sophisticated threats.
- Created the new Baseline rule set of firewall policies to define the optimum security posture of each agency’s boundary protection.

Endpoint Encryption - Successfully implemented full disk encryption to over 10,000 of laptops, desktops, and tablets in 31 agencies, in over 440 locations. having full disk encryption through a centrally managed solution.

Centralized Patch Management - Moved from an ad-hoc patching strategy to a centrally managed solution. This increased compliance with the patch management policy from over 30,000 critical operating system patches missing to less than 10,000 missing across 11,500 machines in the past 30 days. This represents a trend that has continued over the previous 8 months.

Splunk - Provides real-time monitoring of compliance posture and detection of threats and issues in real-time.   Provides one pane / dashboard view of the network environment and systems.

Vulnerability Scanning - Active Vulnerability Scanning ongoing for 19 of 28 Enterprise agencies for laptops, desktops, tablets, and servers, with the remainder of the 28 agencies expected to be in the environment by the end of Q1. Active monitoring of the tools allows the operations team to respond to and remediate these threats with the goal of minimizing the impact to data security and operations.

Security Awareness Training - Launched a campaign to increase the security awareness for state employees.

Cybersecurity Incident Response - Provided support for 11 major incidents. This support prevented proliferation of multiple malware and backdoor compromises.

Web Application Firewall - Over 100 Applications protected by the Department Web Application firewall (WAF). The WAF protected critical maryland.gov websites from over 2,600 buffer overflow attacks, 168,000 SQL injection violations, and 440 cross site scripting attempts in the last month by using the application firewall features of the WAF.

DMARC - In fiscal 2018 we plan to start to roll out DMARC to prevent email Spoofing. (Spoofing is when someone pretends to send an email from someone else. It is a common tactic used by hackers to get people to open an email.)

VIRTRU - Virtru is an email encryption plugin that the State uses to encrypt sensitive emails. Virtru

EMAIL Data Loss Prevention (DLP) - Gmail is capable of using Data Loss Prevention (DLP) to reject messages that aren't securely sent using Virtru. Each sent message is scanned for personally identifiable information (PII) as it leaves the State's email system. If the email contains PII it will be flagged and reported to agency admins.

Email Encryption - G-Suites utilizes end to end encryption. Gmail and Google Drive files are encrypted in as they traverse the internet and when they are stored.

On July 1, 2017, the council released its biennial report. Much of the report addresses issues that are beyond the Department's responsibilities. But the report does have two new fiscal 2017 to 2019 recommendations that could directly affect the Department operations. The council recommends legislation or policy changes that would require State IT procurements to include an independent security verification device or code readiness and/or system security readiness prior to acceptance. This addresses supply chain cybersecurity risks to data and the ability to provide services. The council did recognize that this could impact costs of goods and services as well as the business sector and asked that cost and business considerations be taken into account. The council also recommends that Maryland develop capability for sharing cybersecurity information and providing outreach support. **The Department should be prepared to brief the committees on the council's work and recommendations that affect State agencies.**

There is currently legislation (SB882) being proposed that is proposing the same security verification outlined above.   Our opinion is that it already duplicates other efforts, is somewhat redundant to other legal mechanisms and would essentially add another hurdle to the procurement process. The estimated impact it would have on improving our cybersecurity defenses would be minimal at best.

Cybersecurity professionals have noted that the average employee is often the weakest link. Employees let hackers in by inadvertently providing passwords or loading malware into a system. To prevent against this, the Department introduced a cybersecurity awareness training program in December 2013. The program is delivered to registered Executive Branch employees and contractors with a State email account. It consists of monthly lessons on topics like passwords, working remotely, and data loss prevention. The service is provided by Security Mentor, a web-based training provider. The program was made mandatory by the previous Administration for Executive Branch employees. The training is provided at no cost to the agencies. A measure of employees' awareness is the percent of employees that are compliant with the awareness program. This indicator has declined from 90% in fiscal 2016 to 80% in fiscal 2017. **The Department should be prepared to brief the committees on its employee cybersecurity awareness training programs. This should include a discussion of the availability of the programs and attempts to increase participation.**

An RFP is in place and will address these training programs.

As recent audits and MFR data show, the State is vulnerable to social engineering. Common audit findings reveal that not all agencies are using anti-malware software (insufficient use of technology). Administration rights and excessive network level access (insufficiently limiting information) are also common findings. In addition, MFR data shows that 80% of employees are compliant with the statewide Cybersecurity Awareness Training Program (insufficient staff education), meaning that 20% are not compliant. **The Department should be prepared to brief the committees on its efforts to minimize the risks of social engineering.**

There is currently an RFP in progress for end user security training which will provide awareness training for social engineering.

The audits show that there are policies with which State agencies are struggling to comply. Although agencies are given policy guidance, implementation has been uneven, and there are weaknesses in the State's cybersecurity defenses. **The Department should brief the committees on how it plans to address these weaknesses, especially weaknesses that recur.**

The State of Maryland currently subscribes to the "Federated" model of IT, where each agency not utilizing the Department's shared services is responsible and accountable for their own IT.

While this model gives the individual agency a high level of control and customization it results in varying levels of IT service and cybersecurity defense maturity. the Department recognizes that small and midsize agencies struggle with properly securing their environments. However, the Shared Services plan is designed to alleviate such issues over the next several years provided the agencies choose to participate in the offered services.

Currently the Department establishes security policies for executive agencies. However, the Department does not have the authority to compel compliance with those policies or the means presently to determine compliance with those policies.

This past year we are implementing our service delivery model as a "Shared Services" model.

This means that the Department will now function as an Managed IT Service Provider one would find in the private industry. We are offering our highly secured, and highly available IT services to any State Agencies or local municipalities requesting services from the Department. This is only an offer of services, we are not empowered to mandate this model for non-Executive branch agencies.

DLS is concerned about the stability of staffing for the Maryland Cybersecurity Program. A primary concern about the program is the high vacancy rates. **Exhibit 12** shows that the program has at least three of six positions vacant in 13 of the last 20 months. The State's cybersecurity director recently resigned, and the program's vacancy rate is 44% since the beginning of fiscal 2018. In a January 2018 *Joint Chairmen's Report* (JCR) response, the Department and DBM noted that State IT salaries tend to lag behind other jurisdictions. **The Department should be prepared to brief the committees on the high vacancies in the Maryland Cybersecurity Program and any efforts to keep positions filled.**

The Department has made recommendations to the Department of Budget and Management regarding compensation for these, and all IT positions and DBM is working on these positions.

Beyond the State PINs at our disposal we also have an outside cybersecurity partners who provide cybersecurity services and consulting including our SOC as well as a temporary CISO.

2. Rural Broadband

The Office of Rural Broadband Is Formed: In order to be responsive to concerns about the availability of broadband in rural areas of the State, on August 11, 2017, the Governor signed Executive Order 01.01.2017.14, which created the Office of Rural Broadband in the Department. The office is required to assist local jurisdictions in their improvement of accessing high-speed Internet; identifying and coordinating the delivery of sources of funds, including federal funds specifically identified for this purpose; working with local economic development agencies to identify areas with a demand for better Internet services; investigating new technologies that would increase high-speed Internet availability; and developing policy, regulations, or legislation relevant to increasing broadband availability. The Department has examined several approaches to enhance rural broadband. Affordability also seems to be a concern since some areas with broadband have comparatively low rates of broadband usage. Several agencies are also supporting rural broadband efforts. **To get a comprehensive perspective, DLS recommends that DoIT's Office of Rural Broadband report to the budget committees on the State's rural broadband efforts.**

Agreed**.**

Other State agencies involved with this effort are DHCD, the Maryland Department of Transportation (MDOT), Commerce, and the Maryland Department of Planning (MDP). The order required that these agencies report on their efforts to identify and coordinate resources and technology within 45 days of the signing of the order – this date has already passed and the reports have not been completed. The order also requires that State agencies work with local jurisdictions and other stakeholders, such as the Maryland Broadband Cooperative and the Rural Maryland Council. By April 2018, the office is required to have developed a demonstration project to increase the availability of broadband on both the Eastern Shore and in Western Maryland. **The Department should be prepared to brief the committees on the status of the proposed demonstration project.**

Western Maryland Demonstration Project

Garrett County contains some of Maryland's most rural and sparsely populated communities. Many residents were without access to high speed internet service. This challenge for residents prevents them from effectively communicating with friends and families using modern technologies, prevents them from telework opportunities, and deprives children from educational opportunities at home. Lack of availability of suitable internet service also impairs growth and development of business.

Representatives of Garrett County, including Kevin Null, County Administrator and James Hinebaugh contacted the Hogan Administration for help. These representatives were supported by members of Garrett County's team, including Cheryl DeBerry and Nathaniel Watkins, Garrett County.

Garrett County advised the Hogan Administration of a public private partnership they had developed with Declaration Networks Group (DNG). The goal of this partnership is to positively impact the aforementioned challenges. The partnership is structured such that Garrett

County contributes backbone network infrastructure, and DNG provides delivers internet service to retail customers, utilizing this backbone network infrastructure provided by Garrett County. To further their program, they needed access to space on aerial towers under the custody of the State of Maryland. By gaining access to this tower, which is currently used primarily by MPT, DNG would gain the ability to provide retail services to additional residents.

The Department of Information Technology coordinated stakeholders from a variety of Maryland agencies to make available the tower space required to support the current needs, while also streamlining future access to tower space that Garrett County might need. The intended, and achieved, result is to accelerate Garrett County's efforts to extend service coverage.

Eastern Shore Demonstration Project

A project was identified in Crisfield where Somerset County officials had explored the use of federal disaster relief funding intended to support hurricane Sandy recovery for the construction of fiber optic cable from a library at 100 Collins Street in Crisfield, southwest along Maryland Avenue and Main Street to the peninsula. Importantly, custody of the assets created from this project would have been turned over to the Maryland Broadband Cooperative upon project completion. It was conceptualized by officials with Somerset County, Crisfield, and MDBC, that citizens and private industry could benefit from this expansion. The proposers of the project pointed toward a housing authority complex in Crisfield as a basis for their application to DHCD.

Unfortunately, it was discovered that the funding was incompatible with the County's proposed use due to MDBC inability to work within the federal guidelines established for federal disaster relief funds. At that time the Department of Information Technology proposed that the Department construct a similar expansion of fiber optic cable from the library to the peninsula; however, the fiber constructed would remain under the custody of the Department. the Department plans to make available this fiber infrastructure to outside parties, like MDBC, in a manner consistent with the Department's existing resource sharing agreement program, effectively maintaining the benefits the original proposal had hoped to achieve. As an enhancement to the originally proposed plan, the fiber would be available for use within Maryland government.

The Department has engaged in an effort to build at least one use case, prior to the investment of funds to build the new infrastructure. DNR stepped forward with an expression of interest. DNR's use case would cause the implementation of high speed wireless internet services at Somers Cove Marina, allowing employees to work more efficiently and providing guest Wi-Fi service for visitors, an amenity that DNR believes would have a beneficial economic impact on the marina and surrounding community. the Department has provided estimates to DNR for this wireless implementation, in a tiered structure beginning at $13,000 to cover the marina office. Successive tiers successively increase coverage, with a correspondingly increasing level of investment. DNR has advised the Department that it does not have adequate funding to invest in this wireless infrastructure but is working to identify external sources of funding. the Department has agreed to assist DNR in those efforts.

The Department has performed a procurement and is now commencing the construction of the fiber infrastructure along the above mentioned path. This fulfillment provides benefits to many stakeholders, including: the citizens of Crisfield who, via MDBC and its membership, will increase broadband choices; Somerset County and Crisfield who will receive their envisioned fiber expansion while retaining the opportunity to work with DHCD to utilize the disaster relief funding for other purposes; and the State who will have an expanded footprint to service government agencies in and around Crisfield.

While broadband is available to a majority of Maryland's households, it is not ubiquitous. While some households do not have broadband service because it is unavailable, there are also households without broadband service in areas that have broadband access. In addition to availability, broadband usage is also influenced by cost. **The Department should be prepared to brief the committees on options to expand broadband availability.**

Over 64,000 Marylanders have no access at all to affordable high-speed internet service, and over 339,000 people have either no access or only one provider, which can often be unaffordable. The *Task force on Rural Internet, Wireless and Cellular Service* (Senate Bill 717/House Bill 169 - Connecting Rural Maryland Act of 2017) has issued a number of recommendations. Some of these recommendations contained technical or operational activities, and the Department is prepared to discuss these.

The Department is actively working with its partner agencies to streamline regulations toward an environment more conducive to the growth of rural internet services. For example, the Department has supported a MDE/DNR led initiative to improve the permitting process for new infrastructure build outs. This initiative also includes the Maryland Department of Transportation and the Maryland Historical Trust as co-participants with the Department. It is hoped that this streamlined process will reduce the regulatory burden on private industry and reduce the time to market for new internet services.

The Eastern Shore Regional GIS Cooperative (ESRGC), part of Salisbury University has performed a broadband mapping initiative. This project expired in 2014. Because information technology is inherently volatile, the data provided is aging and is, unfortunately, now of limited use. It has been proposed by the *Task Force* that this data be updated. the Department has previously engaged in discussions with ESRGC to explore strategies for updating this information.

The Department is aware of the Governor's proposal to appropriate funds for rural broadband initiatives and is aware that these funds will be appropriated via DHCD. The DHCD plan intends to utilize DHCD loan programs, grant resources, and the appropriation mentioned above to develop a program to implement the recommendations of the *Task force on Rural Internet, Wireless and Cellular Service* (Senate Bill 717/House Bill 169 - Connecting Rural Maryland Act of 2017). the Department is ready to provide technical expertise in concert with DHCD's financial expertise to develop an organized strategy to maximize this investment in rural broadband.

3. One Stop Portal

The Department is also proposing a deficiency appropriation for a new major IT project to provide a single website that allows the State portal's visitors to search for all State licenses and permits. To fund the One Portal project, the budget includes a $1 million fiscal 2018 deficiency appropriation and $2 million in the fiscal 2019 MITDPF appropriation, with a total project cost of $6 million. Appendix 2 provides specific project detail. **Once deployed, the Department of Legislative Services (DLS) recommends that the Department should track the adoption rate for this project.**

The Maryland Department of Information Technology (DoIT) is working to focus on improving citizen engagement through providing convenient digital transaction and interaction opportunities with Maryland State government.

ONE Portal – A single, intuitive website with a modern design that will allow citizens, residents and visitors to search for all state licenses and permits. The website will incorporate smart search capabilities that will allow people to use natural language to find what they're looking for. It will also allow them to find critical information such as application documentation requirements, cost, approval time, expected completion time, how long the permit/license is valid for, and who to contact just in case they have any additional questions.

Go Paperless – Maryland government currently has over 1,000 forms online spread across state agency web sites. Many of these forms are only available to download and print, and people are required to mail them back in to each respective agency for action. DoIT will focus on modernizing many of these forms by seamlessly integrating digital processing with existing traditional channels, implementing sound design processes through automation to decrease back-and-forth interactions, and developing a broader ecosystem with the goal of eventually providing residents and visitors the means to manage their transactions with state government from one portal.

Modernize Back-End Applications – While it is important to focus on moving government interaction with its citizens to digital channels, it is also equally critical that we also invest in transformation of many of the state's legacy applications that process these transactions. Many of these legacy applications are expensive to maintain and present multiple cybersecurity risks and vulnerabilities due to the utilization of old mainframes and outdated technologies. DoIT will allocate resources to modernizing many of these applications using up to date technology platforms and frameworks. The Agency will focus on standardizing functionality as well as the look and feel of these applications, which will result in additional cost saving for the state in terms of future support and maintenance.

The private sector has moved the vast majority of its customer transactions to customer-facing digital platforms. Many State government agencies still employ more time-consuming, inefficient traditional channels such as face-to-face/over-the-counter service provision, telephone use, and mail interaction. These legacy channels require significantly more time and resources to process and complete than the proposed digital alternatives. They involve interacting with a counter agent, back office staff sorting through mailed-in forms (which can be lost or misplaced), or incomplete paper forms that lack required information or data validation. Digital channel processing, such as employing an online form, are much quicker and easier to use and there is room for significant time and cost savings for both the citizens and government. Increased trust, satisfaction, transparency, citizen engagement and collaboration are the end results.

We will monitor the number of applications filled out online vs. offline as we modernize systems. We will also monitor the number of people viewing the License and Permit website.

4. Shared Services

State Agency Support Indicators Should Change as the 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. As discussed in the Issues section of this analysis, the Department is implementing its Enterprise Tech Support Initiative. **The Department should develop new indicators that reflect its changing workload.**

Agreed, the Department will have new Managing for Results (MFRs) for our FY20 budget request.

In fiscal 2017, the Department reorganized and most of these programs' operations are now performed by ASM and the infrastructure program. ASM now also includes functions like GIS, Google services, and web services. The infrastructure program supports telephone systems, networkMaryland, and State agency IT enterprise operations. The Department has discontinued publishing performance data for these support functions. As discussed in the Issues section of this analysis, the Department is implementing its Enterprise Tech Support Initiative. DLS' concern is that these indicators are out of date. **The Department should develop new indicators that reflect its changing workload, including the Enterprise Tech Support Initiative's workload.**

Agreed, the Department will have new MFRs for our FY20 budget request.

How Will Service Quality Be Measured? Through its service desk, the Department now automatically sends those served a satisfaction rating survey. The Department should also develop measures for these new day-to-day support services that it will be providing and should report these measures with its MFR data provided in the budget. The concern is that service quality could be deteriorating, but the General Assembly would be unaware because there are no reliable measures. How will the Department measure the quality of the services it provides? **The Department should develop MFR indicators that measure service quality.**

Agreed, the Department will have new MFRs for our FY20 budget request.

Enterprise Tech Support Initiative: the Department began migrating day-to-day IT operations in fiscal 2016. Currently, approximately 9,500 State employees are served by the Department. **The Department should develop indicators that measure service quality and prepare a master plan for the Enterprise Tech Support Initiative.**

Agreed. We currently provide a report quarterly to all agencies subscribing to our shared services model. SEE ATTACHED SAMPLE REPORT.

What is the Master Plan? Since fiscal 2017, DJS and DHCD positions have been transferred back into those agencies as tech support services are no longer provided for those agencies. After a period of rapid growth, it appears that the Enterprise Tech Support Initiative is retrenching. **The Department should prepare a master plan for the Enterprise Tech Support Initiative.**

The Department's IT Master Plan incorporates the Enterprise Tech Support Initiatives.

What Will This Cost and What Will Be Saved? the Department anticipates that it will receive a mix of general funds appropriated in its budget and reimbursable funds from other agencies. The Department also anticipates that savings will be realized. As previously discussed, fiscal 2017 costs exceeded budgeted costs by $1.7 million. The Department has not provided any data showing either costs or expenses associated with enterprise technology support. **The Department should prepare a comprehensive report on anticipated costs and savings.**

Agreed. The Department will provide an annual report on the Shared Services initiative. Initial cost savings and or avoidances will come from new shared services agreements that will give agencies the ability to identify their own costs savings with unprecedented transparency and detail. This will allow agencies to better utilize their resources. Specifically, the Department is in the process of developing detailed chargeback models which will for the first time provide agency leadership true visibility into the total cost of ownership of the IT services they consume.

It will provide incentive agencies to temper their demand for IT based services by utilizing this new consumption based funding model. The Shared Services allowed the State to eliminate 64 vacant PINs saving the state approximately 4M annually. The Shared Service model has increased the support to PIN ratio eight-fold, 840%, supporting nearly 10,000 PINs with only 235 PINs compared to 600 PINs supported by 120 PINs previously.

It is encouraging that the State is expanding the number of services that are offered online and that some are being recognized. However, missing from the measures is any indication of the quality of Maryland.gov. There are numerous factors that contribute to a good website, including accessibility, navigation, content, security, speed, accuracy, and currency (up-to-date data). The Department has added an indicator that measures customer satisfaction. **The Department should be prepared to brief the committees on how it evaluates the quality of its websites.**

Security: The Maryland.gov and eGov sites undergoes annual security audits and certification by a 3rd party.

Accessibility: Maryland.gov incorporates accessibility testing when there are major version releases (annually). the Department continues to offer agencies guidelines for meeting the Nonvisual Access (NVA) Guidelines and a website template that meets NVA guidelines. the Department continues to research cost-effective accessibility testing tools that may be leveraged enterprise-wide.

Navigation and speed: The Department review and provides site statistics utilizing Google Analytics that report of website's performance and user's navigation patterns. Maryland.gov site speed averages approximately 4.5 seconds. Our maintenance and operations teams regularly monitor site performance against baseline load times and alerts when there is an increase in load time.

Ensuring content is up to date: The Department’s enterprise web services platform allows agency users (estimated 200 users) to maintain their website content, improving the accuracy and up to date content. The Department provides monthly reports to Enterprise agencies for broken links and provides assistance in updating website content when necessary. Agencies websites not hosted by the Department are contacted as we become aware of any missing content.

Customer Satisfaction is currently measured by surveys. The survey metrics for eGov services is reported in the Department’s MFR statistics, which has an overall satisfaction of 98% in 2018. Additionally, the Department developed the Governor’s Customer Service survey, in collaboration with the Governor’s Office of Performance Improvement, that reports customer satisfaction of executive agencies. Additionally, the Department hosts website surveys for several agencies that collect feedback about agency websites.

5. Data Centers

Status and Future of Data Centers: As IT systems have expanded, the demand to digitally store data has grown. This data is stored in various data centers across the State. Data storage is decentralized in different State agencies. The State does not have a master plan for data centers. **DLS recommends that the Department develop a master plan for data centers. This plan should inventory current assets, project out-year data capacity needs, and compare the benefits of cloud storage compared to the State investing in capacity. Issues to examine with respect to cloud storage or State-built capacity include lifecycle costs, security needs, disaster recovery, and scalability.**

The Department is already in the process of consolidating the data centers for our current customers (31 state agencies). The Department also has spent the last year building a new IT Asset Management (ITAM) program which will inventory all the IT assets under our care. We currently use a combination of on premise and cloud storage depending on the use case and cost effectiveness. We informed DBM of the State's need for increased data center capacity and will be working with them on a long-range funding plan during our FY2020 capital budget submission.

The State does not have a master plan for data centers. **DLS recommends that the Department develop a master plan for data centers. This plan should inventory current assets, project out-year data capacity needs, and compare the benefits of cloud storage compared to the State investing in capacity. Issues to examine with respect to cloud storage or State-built capacity include lifecycle costs, security needs, disaster recovery, and scalability.**

Agreed. See previous comment