Audit Report

Department of Information Technology as a Service Provider

March 2019

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

March 21, 2019

Senator Craig J. Zucker, Co-Chair, Joint Audit Committee
Delegate Shelly L. Hettleman, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) operations as a State information technology enterprise service provider. Our audit included an internal control review of DoIT's enterprise services information technology operations and network. DoIT provides enterprise infrastructure and network resources, systems maintenance, and operates as a service provider to numerous State of Maryland Executive Branch and independent agencies (that is, provides centralized, uniform IT services to certain State agencies).

DoIT maintains the State of Maryland *Information Security Policy* applicable to Executive Branch and independent State agencies; however, DoIT had not updated this policy for almost six years despite new and increasing IT security risks. While DoIT had begun, but not completed, efforts to update the *Information Security Policy*, it had, nonetheless, advised legislative committees that the *Policy* had been updated and issued throughout the Executive Branch of State government.

We also found that DoIT did not have an information technology disaster recovery plan for its enterprise services residing within a hosting data center operated by a third-party data center service provider. Additionally, DoIT had not obtained assurance that adequate information technology security and operational controls existed for the same hosting data center.

Our audit also disclosed that operating system software updates were not applied to numerous network devices in use on DoIT-managed enterprise customer agencies networks and on DoIT-only networks. Additionally, DoIT lacked

procedures for maintaining malware protection controls on enterprise customer agencies' workstations relative to workstation administrative rights assignment and updating certain vulnerable application software products.

DoIT's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the audit by DoIT, and its willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

Background Information

Agency Responsibilities

The Department of Information Technology (DoIT) was established by Chapter 9, Laws of Maryland 2008 effective July 1, 2008. DoIT is responsible for information technology policies, procedures, and standards for the State's Executive Branch agencies and commissions, including publishing and maintaining the State of Maryland *Information Security Policy* and its related security requirements.[1]

DoIT also provides various information technology (IT) enterprise services to customer State agencies on a centralized, uniform basis. As of August 2018, enterprise services provided by DoIT included: Managed Security Services for maintaining agencies networks' firewalls; End User Services for supporting agencies computer workstations, providing malware protection software, encryption and host intrusion prevention system software; and Infrastructure Services for hosting agency virtual servers at a third-party service provider's hosting data center, and managing agencies' onsite and branch locations' local area networks including wireless network segments.

DoIT provided enterprise services to customer State agencies from both within the DoIT agency network, and by using substantial IT hardware and software resources installed at the third-party service provider's hosting data center facility which is located in Baltimore.

DoIT's enterprise services support fundamental daily agency IT activities including Internet and Statewide Intranet access, email, computer server operations, and file sharing. DoIT began providing enterprise services to State customer agencies in February 2015. Additional State agencies became enterprise services customers over time, in a phased approach. As of October 2017, 30 separate State agencies were utilizing enterprise services. The Department of Legislative Services Analysis of the fiscal year 2019 Executive Budget noted that 9,529 employees worked within the State customer agencies receiving DoIT enterprise services.

During implementation of enterprise services to State customer agencies, numerous IT employee positions were transferred from customer State agencies to

[1] By Law, DoIT does not have authority or responsibility for the University System of Maryland, Morgan State University, St. Mary's College, or the Maryland Port Administration. Additionally, Chapter 150 of the Laws of Maryland 2018, effective July 1, 2018, exempts the Maryland Stadium Authority from DoIT's authority or responsibility.

DoIT. According to DoIT's records, between November 2015 and November 2016, 115 customer State agencies' IT employee positions were transferred to DoIT. At the time of these transfers, 7 positions were vacant and 2 positions were abolished. Since the noted transfers, 14 positions were subsequently transferred back to the Department of Juvenile Services and the Department of Housing and Community Development, which discontinued use of certain DoIT enterprise services. Additionally, DoIT has relied, to a significant degree, on a contractor for providing personnel and technical expertise related to varying portions of the aforementioned enterprise services.

According to DoIT's records, fiscal year 2018 expenditures related to supporting the aforementioned enterprise services totaled approximately $21.3 million.

This audit focuses on DoIT's role as an IT enterprise service provider to other State agencies. Our Office also performs a separate fiscal compliance audit of DoIT which includes DoIT's fiscal operations and other functions not related to its enterprise service provider role. Our Office also separately audits the enterprise service customer agencies during which we examine information system security controls in place at the agencies to whom DoIT provides IT services.

Findings and Recommendations

Information Security Policy

Background

The State Finance and Procurement Article of the Annotated Code of Maryland establishes the duties of the Secretary of the Department of Information Technology (DoIT). Under State law, DoIT is responsible for developing, maintaining, revising, and enforcing information technology policies, procedures, and standards.

Historically, DoIT has maintained and published a single comprehensive State of Maryland *Information Security Policy*, with the current version having been published in February 2013. The *Information Security Policy* describes security requirements that Executive Branch and independent State agencies must meet in order to protect the confidentiality, integrity, and availability of State-owned information. Information technology (IT) and IT systems are essential assets of the State of Maryland and vital resources to Maryland citizens. All State agencies, employees, and contractors are responsible for protecting such assets from unauthorized access, modification, disclosure, and destruction. The *Information Security Policy* has historically identified the minimum security requirements necessary for protecting the State's IT assets.

Finding 1
DOIT had not updated the *Information Security Policy* applicable to Executive Branch and independent State agencies for almost six years despite new and increasing IT security risks.

Analysis

DoIT had not updated the *Information Security Policy* applicable to Executive Branch and independent State agencies for almost six years despite new and increasing IT security risks. Our review determined that during 2016 and 2017 DoIT developed a collection of 26 new or updated draft IT security requirements categorized by IT functions, but these had not been finalized and published. DoIT personnel advised us that these new IT security requirements were developed under management personnel who were no longer employed with DoIT and that, as of December 2017, they were under review by existing DoIT management. Subsequently, in December 2018, DoIT management personnel further advised us that the goal was to finalize and publish these new IT security requirements, via a revised *Information Security Policy* in the very near future.

Furthermore, during 2017 and 2018, DoIT advised State legislative committees concerning the State of Maryland cybersecurity policies and represented the new, non-published IT security requirements as the official *Information Security Policy*.

- The April 2017 *Joint Chairmen's Report* required the Judicial Information Systems (JIS) and DoIT to submit a report by November 1, 2017, detailing the current status of the State's cybersecurity policies and the feasibility of creating and adopting a unified cybersecurity policy for the Executive and Judicial branches. In response, DoIT advised the Senate Budget and Taxation Committee and House Appropriations Committee, in part, that DoIT maintained 26 separate policies for cybersecurity that were tied to the Federal National Institute of Standards and Technology Cybersecurity Framework. These policies were the same IT security requirements which DoIT management personnel advised us had not been finalized and published and hence were not yet official.

- During the 2017 and 2018 Legislative Sessions as part of its fiscal year 2018 and 2019 operating budget hearings, DoIT advised pertinent State Senate and House Committees that the new, non-published security requirements comprising the *Information Security Policy* and were issued throughout the Executive Branch of State government.

Without updated information security requirements, State agencies were not assisted in addressing the increasing security risks arising from new information system technologies and security threats. According to industry literature, for the almost six-year period since the *Information Security Policy* was last updated (February 2013), IT security risks have grown in scope and at an increasing rate with industry groups recognizing the increased risks related to IT security. For example, the National Association of State Chief Information Officers' (NASCIO's) annually surveys state CIOs to identify and prioritize the top IT policy and technology issues facing state governments, and publishes a related annual Top Ten Priorities list. For each year from 2015 to 2018, the described NASCIO IT surveys ranked IT Security and Risk Management as the number one priority among all state CIOs.

Recommendation 1
We recommend that DoIT

a. complete its review of the draft IT security requirements and finalize an updated State of Maryland *Information Security Policy* in a timely manner;

b. publish and disseminate the updated *Policy* with related implementation guidance;
c. advise the budget committees that the previously described *Policy* updates did not occur, and when the updated *Policy* is subsequently finalized and issued; and
d. develop procedures to periodically update the *Policy*, on an as needed and timely basis.

Information Systems Security and Control

Finding 2
DoIT did not have an information technology disaster recovery plan (DRP) for its third-party operated enterprise services hosting data center to aid in the recovery of related information systems operations.

Analysis
DoIT did not have an information technology DRP for its third-party operated enterprise services hosting data center to aid in the recovery of computer operations from disaster scenarios (for example a fire). DoIT utilized a third-party data center service provider to host portions of its enterprise services operations. A substantial number of DoIT enterprise services servers, supporting network devices, and related Statewide network connections existed within DoIT's enterprise services hosting data center. According to DoIT's enterprise services records as of August 2018, 24 State customer agencies were fully using DoIT enterprise services which were operating on this third-party hosted data center's infrastructure, and 8 other State customer agencies were partially using some form of the aforementioned hosted enterprise services.

The State of Maryland *Information Technology Disaster Recovery Guidelines* for State agencies provide minimum required elements needed for a DRP. Examples of minimum required elements include alternate site processing arrangements, required hardware and software components, and restoring network connectivity. DoIT's disaster recovery plan for State enterprise services would need to incorporate and rely upon some portion of the third-party data center hosting service provider's own DRP.

Without a complete and tested DRP, a disaster could cause significant delays (for an undetermined period of time) in restoring information systems operations for over 30 State enterprise services customer agencies, beyond the expected delays that would exist in a planned recovery scenario.

Recommendation 2
We recommend that DoIT develop and implement a comprehensive DRP, including related testing, to cover all of its enterprise services information technology operations, incorporating and relying on the third-party data center hosting provider's DRP as needed, in order to comply with the requirements identified in the *Information Technology Disaster Recovery Guidelines*.

Finding 3
DoIT lacked assurance that adequate information technology security and operational controls existed over its State enterprise services operations hosted by its third-party data center hosting service provider.

Analysis
DoIT lacked assurance that adequate information technology security and operational controls existed over its State enterprise services operations hosted by its third-party data center hosting service provider, under a contract effective September 8, 2014 through September 17, 2019. DoIT's contract did not require the service provider to obtain an independent security assurances report such as a System and Organization Controls (SOC) report. As of September 2017, DoIT had not obtained a SOC report or any other similar independent security assurances report from the service provider.

After our inquires, DoIT contacted the service provider and found that the service provider had a SOC 2 Type 2 review performed, with a related report issued on December 12, 2016, covering the period of November 1, 2015 to October 31, 2016. In response to our request, DoIT obtained the SOC report from the service provider. Our review of the report disclosed that it identified seven control weaknesses for the service organization's system description and the suitability of the design and operating effectiveness of controls, but the control issues pertained to the hosting service provider's data centers in locations other than the Baltimore location.

The American Institute of Certified Public Accountants has issued guidance concerning examinations of service providers. Based on this guidance, service providers may contract for an independent review of controls and resultant independent auditor's report referred to as a SOC report. There are several types of SOC reports, with varying scopes and levels of review and auditor testing. One type of report, referred to as a SOC 2 Type 2 report, contains the service organization's description of its system and the results of the auditor's examination of the suitability of the system design, operating effectiveness for the

period under review, and can include an evaluation of system security, data availability, processing integrity, confidentiality, and privacy trust criteria. Due to the significance of the State enterprise hosting service provided at the third-party provider's data center, it is necessary that DoIT obtain and review a periodic SOC 2 Type 2 report covering the service provider's operations.

Recommendation 3
We recommend that DoIT

a. **ensure that future enterprise services contracts include provisions requiring third-party service organizations to annually obtain SOC 2 Type 2 reviews for DoIT's outsourced services, and**
b. **obtain and review these SOC 2 Type 2 reports and take appropriate action to ensure that all critical operational and security-related controls are properly addressed.**

Finding 4
Operating system software updates were not applied to network devices in use on DoIT-managed customer agencies' networks and on DoIT-only networks.

Analysis
Operating system software updates were not applied to network devices used on DoIT-managed customer agencies' networks and on DoIT-only networks. According to DoIT's enterprise services records as of August 2018, 30 State customer agencies were receiving network device management services.

- DoIT lacked procedures for updating operating system software for network devices within managed customer agency networks and DoIT's own infrastructure network segments. DoIT personnel advised that formal procedures did not exist for ensuring that managed network devices were running the most current version of the network device operating system software in order to reduce risk related to such devices having software-related security vulnerabilities.

- Our November 2017 test of 10 customer agency and/or DoIT network devices disclosed that 8 of the 10 network devices had outdated operating system software installed with 4 of these devices running a software version that was no longer supported by the device manufacturer. Additionally, we determined from DoIT's enterprise network device management console server records that 101 other DoIT managed network devices were operating using the same outdated operating system software identified during our test. As of

September 2017, records from an enterprise network device management console server identified 1,363 network devices under DoIT management.

When questioned, DoIT personnel advised us that, upon assuming initial responsibility for certain agencies' network devices, it was determined that certain network devices' installed operating system software was already no longer supported by the manufacturer.

Accordingly, all of the DoIT-managed enterprise customer agency and DoIT network devices, including those operating with outdated or unsupported operating system software, were subject to increased security risks from software vulnerabilities and possible related attacks, which could potentially result in disruption of critical network services. The State of Maryland *Information Security Policy* states that system hardening procedures shall be created and maintained to ensure up-to-date security best practices are deployed at all levels of IT systems (operating systems, applications, databases, and network devices).

Recommendation 4
We recommend that DoIT, for managed enterprise network devices' operating system software,

a. identify all critical network devices with obsolete operating system software (no longer supported by the manufacturer) and develop a plan to migrate those devices to manufacturer-supported operating software;
b. develop procedures to regularly identify software updates necessary to eliminate significant security or operational vulnerabilities; and
c. ensure that all managed network devices operate with current vendor supported versions of operating system software, and apply updates for the operating system software in a timely manner.

Finding 5
DoIT's enterprise services operation lacked procedures for maintaining malware protection controls on customer agencies' workstations relative to workstation administrative rights assignment and updating certain vulnerable application software products.

Analysis
DoIT's enterprise services operation lacked procedures for maintaining malware protection controls on customer agencies' workstations relative to administrative rights assignment and updating certain vulnerable application software products.

- DoIT did not properly control the assignment of local administrative rights on enterprise services customer agencies' workstations. We were advised by DoIT personnel that their enterprise services policy was to not assign local administrative rights on managed customer agency workstations to non-IT personnel. However, our review of DoIT procedures as of November 2017 determined that a formal policy for controlling administrative rights defined on customer agency workstations did not exist. Furthermore, related control procedures did not exist, including reviewing employee workstations to identify all administrative rights previously assigned before agencies became enterprise services customers, removing such administrative rights that are not needed, and maintaining schedules of customer agency employees needing assignment of the rights on an authorized exception basis.

  Administrative rights are the highest permission level that can be granted to users and allow users to install software and change configuration settings. If these customer agencies' workstations were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights.

- DoIT supported customer agencies' workstations had not been updated with the latest releases for three application software products that are known to have ongoing security-related vulnerabilities. Vendors for these software products frequently provide software patches to address these vulnerabilities; however, DoIT personnel advised us that, as of December 2017, customer agencies' workstations were not being regularly updated with these software patches. Accordingly, the DoIT managed agencies' workstations running these applications were subject to increased security risks from attacks focused on the related vulnerable applications software.

We review DoIT's results for controlling administrative rights and updating vulnerable application software during our separate State agency audits of many enterprise customers. Since November 2015, we have audited five State customer agencies that used DoIT enterprise services, with each agencies' information system security controls being examined. During the audit of three of these five agencies, we found reportable conditions related to the failure to properly control the assignment of administrative rights and/or the failure to promptly update vulnerable software products.

Recommendation 5

We recommend that DOIT, for its enterprise services managed customer agencies' workstations

a. **limit the assignment of administrative rights on workstations to system and network administrators and those users specifically requiring such rights to perform their job functions, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether such rights are still needed; and**
b. **ensure that all workstations are promptly updated with software patches issued by vendors for recognized vulnerable software products to address known vulnerabilities.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Department of Information Technology (DoIT) as a Service Provider. Fieldwork associated with our audit of DoIT was conducted during the period from August 2017 to December 2017. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine DoIT's internal control over its enterprise services information technology operations and network, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of significance and risk. The areas addressed by the audit included procedures and controls over the enterprise services network infrastructure security and data center hosting. Our audit included an assessment of the security controls for enterprise malware protection management and software maintenance for enterprise devices. The audit also assessed DoIT's procedures for enterprise disaster recovery and maintenance of the State of Maryland *Information Security Policy*.

Our audit did not include DoIT's fiscal operations related to its information technology enterprise services or the computer operations of DoIT as it relates to services primarily received by DoIT itself as an enterprise services customer. DoIT's fiscal operations and own use of its enterprise services are audited separately as part of our fiscal compliance audit of DoIT. At this report's publication, the latest report that covered DoIT's fiscal compliance audit was issued on September 12, 2016. Our audit also did not include certain provided enterprise support services involving network.Maryland and the State's office productivity software suite. These support services are also included within the scope of our audit of DoIT fiscal compliance operations.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DoIT's operations.

We also extracted data from a DoIT network device management system for the purpose of testing network device software updating. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

DoIT's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records; effectiveness and efficiency of operations, including safeguarding of assets; and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect DoIT's ability to operate its enterprise services effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to DoIT that did not warrant inclusion in this report.

DoIT's response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the DoIT regarding the results of our review of its response.

APPENDIX

LARRY HOGAN
Governor
BOYD K. RUTHERFORD
Lieutenant Governor

MICHAEL G. LEAHY
Secretary
LANCE SCHINE
Deputy Secretary

Department Of INFORMATION TECHNOLOGY

State of Maryland
Department of Information Technology

March 19, 2019

Gregory A. Hook, CPA
Legislative Auditor
301 W. Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Hook:

The Department of Information Technology (DoIT) has received the fiscal compliance audit submitted by the Department of Legislative Services, Office of Legislative Audits, dated March 4, 2019. This audit included an internal control review of DoIT's enterprise services information technology operations and network.

DoIT acknowledges the efforts of the legislative auditors during this audit. Responses to the audit findings are attached to this cover letter.

Sincerely,

Michael G. Leahy
Secretary, Department of Information Technology

Responses to Findings and Recommendations

Information Security Policy

Finding 1
DOIT had not updated the *Information Security Policy* applicable to Executive Branch and independent State agencies for almost six years despite new and increasing IT security risks.

Office of Legislative Audits Recommendation 1
We recommend that DoIT

a. complete its review of the draft IT security requirements and finalize an updated State of Maryland *Information Security Policy* in a timely manner;
b. publish and disseminate the updated *Policy* with related implementation guidance;
c. advise the budget committees that the previously described *Policy* updates did not occur, and when the updated *Policy* is subsequently finalized and issued; and
d. develop procedures to periodically update the *Policy*, on an as needed and timely basis.

DoIT Response to Recommendation 1
DoIT agrees with the recommendations and is taking corrective actions as noted below.

a. The updated State of Maryland Information Security Policies have completed an initial legal review and are undergoing revisions as a part of an outreach campaign to solicit feedback and ensure alignment with agency business practices. This outreach campaign is expected to reduce the time and effort associated with dissemination and implementation, once published. The updated policies contain substantially more implementation guidance than previously found in State security policy; this implementation guidance is adapted from guidance from the National Institutes of Standards and Technology (NIST) for implementing similar standards in federal government. The updated policies are expected to be finalized and published second quarter of CY2019.
b. As noted in response to recommendation "1a", we are expecting to finalize and publish the updated policies by the second quarter of CY2019. At that time, the updated policies will also be disseminated to Executive Branch and independent State agencies, as applicable. As noted in response to

recommendation "1a", the policies contain relevant implementation guidance.

c. ***DoIT acknowledges that the previously described policy updates did not occur and agrees to advise the budget committees of this. Once finalized, DoIT will also provide a copy of the updated Policy.***
d. ***The updated policies are to be reviewed on a yearly basis and updated as needed based on findings made during the review cycle or as otherwise deemed necessary by DoIT. These reviews will be documented and maintained for future reference.***

Information Systems Security and Control

Finding 2
DoIT did not have an information technology disaster recovery plan (DRP) for its third-party operated enterprise services hosting data center to aid in the recovery of related information systems operations.

Office of Legislative Audits Recommendation 2
We recommend that DoIT develop and implement a comprehensive DRP, including related testing, to cover all of its enterprise services information technology operations, incorporating and relying on the third-party data center hosting provider's DRP as needed, in order to comply with the requirements identified in the *Information Technology Disaster Recovery Guidelines*.

DoIT Response to Recommendation 2
DoIT acknowledges that the Disaster Recovery Plan (DRP) in effect at the time of the audit did not adequately address all of the requirements identified in the aforementioned guidelines. At the time of the audit DoIT was circulating a revised version of its DRP for comment which addressed many of the items identified by the auditors such as, the increased importance of our data center for hosting agency applications and data, the formalized processes for activating our secondary data center in the event of a disaster, the restoration priority assigned to critical applications and data, and test procedures. DoIT did provide a draft of the revised plan to the auditors during the time of the audit. DoIT expects the updated DRP will be approved and implemented during the second quarter of 2019. This DRP will comply with the requirements identified in the Information Technology Disaster Recovery Guidelines. Testing of the DRP will occur consistent with requirements in the Information Technology Disaster Recovery Guidelines.

Finding 3
DoIT lacked assurance that adequate information technology security and operational controls existed over its State enterprise services operations hosted by its third-party data center hosting service provider.

Office of Legislative Audits Recommendation 3
We recommend that DoIT

a. **ensure that future enterprise services contracts include provisions requiring third-party service organizations to annually obtain SOC 2 Type 2 reviews for DoIT's outsourced services, and**
b. **obtain and review these SOC 2 Type 2 reports and take appropriate action to ensure that all critical operational and security-related controls are properly addressed.**

DoIT Response to Recommendation 3
DoIT agrees with the recommendations and is taking corrective actions as noted below.

a. ***DoIT's current contract for third-party hosting is due to expire in September 2019. DoIT will ensure that all future contracts for third-party hosting services will require the service provider to annually obtain a SOC 2 Type 2 audit and to provide DoIT a copy of the SOC 2 audit within 30 days of it being provided to the service provider. All SOC 2 audits received will be reviewed to ensure the sufficiency of controls. Appropriate action will be taken as necessary. All such reviews and follow-up actions needed will be documented.***
b. ***DoIT has received a copy of the provider's most recent SOC 2 audit (dated December 2018) and has reviewed the report to ensure the sufficiency of controls. DoIT has documented its review. No deficiencies were noted at the Baltimore location. DoIT will continue to request a copy of the provider's related SOC 2 audit(s) that cover the period of the contract term and will conduct a documented review to ensure adequate information technology security and operational controls existed over its State enterprise services operations.***

Finding 4

Operating system software updates were not applied to network devices in use on DoIT-managed customer agencies' networks and on DoIT-only networks.

Office of Legislative Audits Recommendation 4
We recommend that DoIT, for managed enterprise network devices' operating system software,

a. identify all critical network devices with obsolete operating system software (no longer supported by the manufacturer) and develop a plan to migrate those devices to manufacturer-supported operating software;
b. develop procedures to regularly identify software updates necessary to eliminate significant security or operational vulnerabilities; and
c. ensure that all managed network devices operate with current vendor supported versions of operating system software, and apply updates for the operating system software in a timely manner.

DoIT Response to Recommendation 4
As outlined in the Background Information and in the analysis of the finding, between 2015 - 2017 DoIT assumed responsibility for the IT operations of 30 Executive branch agencies. In assuming that responsibility, DoIT assumed the legacy network infrastructure in place at the time. A number of the assumed network devices were end-of-life and end-of-support, running on operating system software no longer being supported by the manufacturer. DoIT agrees generally with the auditors recommendations that DoIT should identify these devices, develop a plan to either replace these devices or upgrade the operating system software with supported versions, and implement processes to ensure software is patched. In circumstances where replacement or updates would negatively impact the functionality of systems that depend upon these devices, DoIT should identify and develop other compensating controls, where possible, to mitigate associated risk. DoIT is addressing the above recommendations as follows:

a. DoIT is aware of critical network devices with obsolete operating system software and has developed two paths to fund the replacement of those devices which are end-of-life. DoIT has established a MITDP to modernize its voice and data infrastructure at a number of locations throughout the State. As a component of that project, DoIT is upgrading network switching appliances that are incapable of supporting Power Over Ethernet (POE). This represents a subset of the network appliances that require replacement. In addition, our FY2020 budget includes funds to replace 20% of the legacy switches deployed at DoIT supported agencies. We believe that these two sources of funding will allow us to remediate all end-of-life switches by the end of calendar year 2020.
b. DoIT is in the process of replacing its current device monitoring software with a product that is capable of detecting all devices, the version of

operating system that they are running, whether or not they are running on a supported operating system, and whether they are patched and include the most current vendor supported versions of the operating system software. The new product will also support the patching and software updates of these devices.

c. *After implementation of this device monitoring software, DoIT will be able to identify all devices representing a risk and will be able to patch and update software on those devices within the managed network which are on supported systems. As mentioned above, updates will be applied in a timely manner, as feasible. Where updates are determined to have a negative impact on the functionality of related systems, an effort will be taken to identify and develop other compensating controls, where possible, to mitigate associated risk.*

Finding 5
DoIT's enterprise services operation lacked procedures for maintaining malware protection controls on customer agencies' workstations relative to workstation administrative rights assignment and updating certain vulnerable application software products.

Office of Legislative Audits Recommendation 5
We recommend that DOIT, for its enterprise services managed customer agencies' workstations

a. **limit the assignment of administrative rights on workstations to system and network administrators and those users specifically requiring such rights to perform their job functions, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether such rights are still needed; and**
b. **ensure that all workstations are promptly updated with software patches issued by vendors for recognized vulnerable software products to address known vulnerabilities.**

DoIT Response to Recommendation 5
DoIT assumed operational responsibility of a number of State agencies during the period 2015 - 2017. Prior to assuming responsibility, DoIT performed an assessment of the state of each agency's IT infrastructure and corresponding operations. This assessment identified deficiencies and developed specific plans for remediating the most significant deficiencies. For all other issues, DoIT developed longer-term plans to triage these deficiencies with the ultimate goal of migrating the agency's infrastructure and operations to a more secure operating environment known as "the fort". Standard PC images, more

hardened firewall rules, and "least privileged access" are all components of the fort.

Regarding the specific recommendations made related to this finding, DoIT has taken the following corrective actions:

a. DoIT also recognizes the occasional need for agency personnel to have shared and/or privileged access to workstations, for instance, in times of emergency response. DoIT is establishing a process for the justification and approval of such requests, to be evaluated based on a legitimate business need, balanced with security and operational risk. Agencies will be expected to internally comply with this procedure by verifying that the business need is justified and the associated risks are deemed acceptable to that agency.

Administrative rights, and more specifically the granting and management of local administrative rights, was an area where the processes employed by the agencies prior to DoIT assuming responsibility varied greatly. DoIT has addressed the most egregious instances identified in its assessments, but acknowledges that there is still work to be done to get each agency to a status where least privileged access and the processes to support it are in place.

DoIT has begun a more extensive discovery and review of local administrative rights. Each instance will be vetted to identify whether or not a legitimate business need exists for the user rights. Where a legitimate business need exists, it will be documented as an exception. Where a business need does not exist, it will be removed. We expect to have this work completed by end of calendar year 2019.

Once this project has been completed and going forward, DoIT will establish procedures so that a periodic review will be conducted to determine administrative rights have been properly assigned. This review will be documented and maintained for future reference.

b. DoIT acknowledges that operating system and application patching of workstations significantly enhances the State's security posture. It is for this reason that DoIT has expended considerable resources improving our processes and procedures. At the time of the audit, DoIT had improved patching significantly in relation to what was inherited. As of this response DoIT's workstations are now 99.81% compliant in relation to critical operating system patches. With processes in place to support operating system compliance, we are now identifying and addressing vulnerabilities in

regards to specific off-the-shelf applications. In many instances, uninstalling legacy applications that are no longer being used will resolve the vulnerability. In other instances, replacing a legacy application with a functionally equivalent product which is better supported will resolve the issue. While we are working to address all vulnerabilities, there is a subset which cannot be addressed because of how they are used by custom-developed legacy applications. These issues will have to be addressed by either replacing/re-writing the application or by implementing compensating controls to reduce the vulnerability.

Going forward and as noted in the response to recommendations for finding 4, DoIT is in the process of replacing its current device monitoring software with a product that is capable of detecting all devices and whether they are patched with the most current versions. The new product will also support the patching updates of these devices to ensure that updates will occur in a timely manner, when appropriate.

AUDIT TEAM

R. Brendan Coffey, CPA, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

J. Gregory Busch, CISA
Information Systems Senior Auditor

Roman J. Gouin
Justin P. Vlahacos
Information Systems Staff Auditors