Audit Report

# Comptroller of Maryland
# Information Technology Division
# Annapolis Data Center Operations

July 2020

**OFFICE OF LEGISLATIVE AUDITS**
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

## Joint Audit and Evaluation Committee

Senator Clarence K. Lam, M.D. (Senate Chair)
Senator Malcolm L. Augustine
Senator Adelaide C. Eckardt
Senator George C. Edwards
Senator Katie Fry Hester
Senator Cheryl C. Kagan
Senator Benjamin F. Kramer
Senator Cory V. McCray
Senator Justin D. Ready
Senator Craig J. Zucker

Delegate Carol L. Krimm (House Chair)
Delegate Steven J. Arentz
Delegate Mark S. Chang
Delegate Andrea Fletcher Harrison
Delegate Keith E. Haynes
Delegate Michael A. Jackson
Delegate David Moon
Delegate April R. Rose
Delegate Geraldine Valentino-Smith
Delegate Karen Lewis Young

## To Obtain Further Information

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

## To Report Fraud

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.

## Nondiscrimination Statement

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the United States Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

July 27, 2020

Senator Clarence K. Lam, M.D., Senate Chair, Joint Audit and Evaluation Committee
Delegate Carol L. Krimm, House Chair, Joint Audit and Evaluation Committee
Members of Joint Audit and Evaluation Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Comptroller of Maryland – Information Technology Division (ITD). ITD operates the Annapolis Data Center which provides computing and network resources and operates as a computer services bureau for the Comptroller of Maryland and other customer agencies. This audit represents the second of two fiscal compliance audits of the ITD and consists of an internal control review of the data center and network administered by ITD. Our audit did not include ITD's fiscal operations which are separately audited by us and reported upon in an audit report of the same name.

Our audit disclosed that sensitive personally identifiable information (PII) was maintained in a manner that did not provide adequate safeguards and made the information more vulnerable to improper disclosure. This sensitive PII involved mainframe-based data within approximately 12,496,000 records.

Additionally, we found that mainframe security software access and monitoring controls were not adequate, with reporting and monitoring controls over database management software also not being adequate.

Our audit also disclosed that network-based intrusion detection prevention system (IDPS) coverage did not exist for untrusted traffic entering the ITD data center network from certain origin points, and the Comptroller of Maryland's mobile computers did not utilize a host-based firewall. In addition, our audit determined that security risks existed for the Comptroller network's information technology (IT) resources because a group of 57 IT Contractors working on a large systems project had unnecessary network-level access to the network.

Finally, our audit included a review to determine the status of the three findings contained in our preceding audit report. We determined that ITD satisfactorily addressed one of these findings. The remaining two findings are repeated in this report.

The Comptroller of Maryland's response to this audit, on behalf of ITD, is included as an appendix to this report. In accordance with State law, we have reviewed the response and noted that ITD disagrees with certain of the report's findings, while the nature of other responses, in which there is agreement, require further clarification. In each instance, we reviewed and reassessed our audit documentation, and reaffirmed the validity of the finding. Consequently, we believe ITD's disagreement has no merit and is contrary to current State information technology security policy. In accordance with generally accepted government auditing standards, we have included "auditor comments" within ITD's response to explain our position. We will advise the Joint Audit and Evaluation Committee of any outstanding issues that we cannot resolve with ITD.

We wish to acknowledge the cooperation extended to us during the audit by ITD. We also wish to acknowledge the Comptroller's and ITD's willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

# Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

# Background Information

## Agency Responsibilities

The Information Technology Division (ITD) operates the Annapolis Data Center as a computer service bureau, and all operating costs are reimbursed by user agencies that are charged for services performed.  ITD also develops and maintains application systems for agencies under the Comptroller of Maryland and provides data center disaster recovery capabilities.  Additionally, ITD maintains the mainframe operating system and security software environment in which many agency applications are executed.  While retaining operational responsibility, ITD relocated the mainframe computer to a Baltimore hosting location during December 2018.  Some of the applications supported by ITD include the Maryland State Integrated Tax System, the State Payroll System, the Maryland State Financial Management and Information System, and the State's Medical Care Programs Administration (Medicaid) System.

ITD operates an internal network that provides services, including internet and Statewide intranet access, email, and file sharing, to all the divisions of the Comptroller of Maryland.  According to the State's records, ITD fiscal year 2019 expenditures totaled $40.5 million.

## Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the three findings contained in our preceding audit report dated March 31, 2015.  As disclosed in the following table, we determined that ITD satisfactorily addressed one of these findings.  The remaining two findings are repeated in this report.

### Status of Preceding Findings

| Preceding Finding | Finding Description | Implementation Status |
|---|---|---|
| Finding 1 | Mainframe security software access and monitoring controls were not sufficient. | **Repeated**<br>(Current Finding 2) |
| Finding 2 | Contractors had unnecessary network-level access to the Comptroller's network. | **Repeated**<br>(Current Finding 4) |
| Finding 3 | Controls over the Comptroller's Data Loss Prevention System need improvement. | Not Repeated |

# Findings and Recommendations

## Sensitive Personally Identifiable Information (PII)

**Finding 1**
**The Information Technology Division (ITD) maintained sensitive PII in a manner that did not provide adequate safeguards.**

**Analysis**
ITD maintained sensitive PII in a manner that did not provide adequate safeguards. ITD supported computer operations for multiple mainframe applications, which processed such sensitive information, but without adequate safeguards. For example, on February 21, 2019, we noted that one application's mainframe database contained sensitive PII involving approximately 12,496,000 records, and was maintained in a manner that made the information vulnerable to improper disclosure. ITD personnel advised us that this sensitive PII was subject to other substantial mitigating controls; however, our review determined these controls were not comprehensive. Detailed sensitive aspects of this finding were omitted from this report, however the related detailed information was previously shared with ITD for purposes of implementing the following recommendations.

The State of Maryland *Information Technology Security Manual* requires that agencies protect confidential data using adequate safeguards and/or other substantial mitigating controls.

**Recommendation 1**
**We recommend that ITD implement appropriate information security safeguards for sensitive PII it maintains.**

## Mainframe Software

**Finding 2**
**Controls involving access and monitoring over mainframe security software as well as database software reporting controls were not adequate.**

**Analysis**
Controls involving access and monitoring over mainframe security software, and reporting and monitoring over database management software were not adequate.

- Groups of 3 to 34 unique accounts involving either ITD or Department of Information Technology (DoIT) personnel had unnecessary direct unlogged or logged access to 12 categories of critical operating system and other system software production files. For example, for 10 of the 12 files' categories, this access was granted to at least 19 separate accounts, with a subset of 3 of the files' categories being defined such that the unnecessary access was granted to 34 separate accounts. Accordingly, unauthorized changes could occur to these production files causing inappropriate changes to production data, which in some cases could go undetected. A similar condition was commented upon in our two preceding audit reports.

- Reviews of security software violation logs pertaining to critical production systems data files lacked needed controls. As of June 4, 2019, reviews for one category of violation logs involving a tax-related system were not performed after November 8, 2017. For a second category of violation logs separate from the tax-related system, ITD's log reviews only focused on activity by certain ITD personnel, with no reviews made for other activity. Accordingly, there was a lack of assurance as to the propriety of the changes made to critical files. A similar condition was commented upon in our two preceding audit reports.

- Activity reporting of changes made to critical database management software catalog tables were not generated, despite ITD having a software product capable of producing such information. Catalog tables for database software record a variety of authorization values for overall database content, users, and privileges. As such, unauthorized and/or inappropriate activities affecting the integrity of the database information could go undetected by management.

**Recommendation 2**
**We recommend that ITD**

**a. restrict access to critical operating and system software files to only those individuals requiring such access and log all such accesses (repeat);**
**b. ensure that the review of security software violation logs includes activity for all time periods and for all users (repeat); and**
**c. implement activity reporting for changes made to critical database management software catalog tables, review such reports for propriety, document these reviews, and retain the reviews for future reference.**

## Network Security

**Finding 3**
**Network-based intrusion detection and prevention system (IDPS) coverage did not exist for traffic flowing into the ITD network from certain origin points, and the Comptroller of Maryland's mobile computers did not utilize a host-based firewall.**

### Analysis

Network-based IDPS coverage did not exist for untrusted traffic entering the ITD data center network from certain origin points, and the Comptroller of Maryland's mobile computers did not utilize a host-based firewall.

- Network-based IDPS inspection coverage did not exist for traffic entering the ITD network over a mainframe internet connection, the Statewide intranet connection, and for traffic flowing from a neutral network zone to a database server network segment. The absence of IDPS coverage for such traffic entering the ITD network creates network security risk, as such traffic could contain undetected malicious data.

  The State of Maryland *Information Technology Security Manual* requires protection against malicious code and attacks by using IDPS coverage to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information. Strong network security uses a layered approach, relying on various resources, and is structured according to assessed network security risk. Properly configured IDPS protection can aid significantly in the detection/prevention of, and response to, potential network security breaches and attacks.

- The Comptroller of Maryland's laptop computers did not have host-based firewalls enabled. ITD personnel advised us that the Comptroller's IT security policy did not include enabling the host-based firewall on laptop computers, and a limited test of five laptop computers during June 2019 confirmed that they did not have an enabled host firewall. ITD personnel advised us that as of June 17, 2019, approximately 600 laptops were in use within the Comptroller's offices. If these laptops were used outside of the Comptroller network locations, those without such firewalls would be susceptible to attack from untrusted traffic.

  The State of Maryland *Information Technology Security Manual* requires that information systems control information flows within systems and between interconnected systems using boundary protection devices such as firewalls that employ rule sets to provide a traffic filtering capability.

**Recommendation 3**
**We recommend that ITD**

a. **ensure that IDPS protection exists for all traffic from untrusted sources entering the ITD network flowing to critical servers and network segments within the data center, and**
b. **work in conjunction with the Comptroller of Maryland's various divisions and units to ensure that all Comptroller laptop computers are protected by an enabled and properly configured host-based firewall.**

### Finding 4
**Security risks existed from information technology (IT) contractors having unnecessary network-level access to the Comptroller's network.**

**Analysis**
Security risks existed from IT contractors having unnecessary network-level access to the Comptroller's network, despite certain indirect security measures implemented. The Comptroller had a significant development project in progress to replace multiple existing systems and as of July 17, 2019 the vendor working on the project employed 57 IT contractors. These 57 IT contractors had unnecessary network level access to almost all of the Comptroller's network versus access to only the Comptroller network devices and ports required to perform their contractual duties, which involved certain productivity resources, such as email, printers, and some shared storage. ITD had implemented certain general measures related to these contractors involving assignment of Comptroller workstations, network accounts, and some security policies to help protect its network from these contractors. However, the unnecessary access occurred because the IT contractors' remote and onsite Comptroller network traffic was not subject to any filtering.

The State of Maryland *Information Technology Security Manual* requires an authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concept of least privilege allowing only authorized access to accomplish assigned tasks.

A similar condition was commented upon in our two preceding audit reports.

**Recommendation 4**
**We recommend that ITD restrict IT contractors' network-level access within the Comptroller network to only those servers and workstations necessary for them to perform their duties (repeat).**

# Audit Scope, Objectives, and Methodology

We have audited the Comptroller of Maryland – Information Technology Division (ITD). Fieldwork associated with our general controls audit of ITD's data center was conducted during the period from March 2019 to June 2019. Additionally, fieldwork associated with our audit of the network was conducted during the period from April 2019 to July 2019. 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 ITD's internal control over ITD's data center and network and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support the Comptroller and ITD data center user agencies. Specifically, given ITD's widespread responsibility for the Comptroller network, our audit included an evaluation of the security control environment for all portions of the Comptroller network controlled by ITD.

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 mainframe operating system, security software, and critical databases. Our audit also included an assessment of the security controls for critical routers, firewalls, switches, and virtual private network appliances, as well as an assessment of the security controls related to ITD's wireless connectivity and the use of anti-malware software to protect the Comptroller's computers. We also determined the status of the findings included in our preceding audit report.

Our audit did not include ITD's fiscal operations which are audited separately within an ITD fiscal operations audit report. The most recent fiscal compliance report that covered ITD's fiscal operations was issued on November 13, 2017.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of ITD's operations, and certain tests to evaluate the effectiveness of controls. We also 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.

ITD'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 security for the Comptroller's data center and network and compliance with applicable laws, rules, and regulations are achieved. As provided in *Government Auditing Standards*, there are five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Each of the five components, when significant to the audit objectives, and as applicable to ITD, were considered by us during the course of this audit.

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 ITD's ability to operate 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 ITD that did not warrant inclusion in this report. Aspects of certain findings contained in this report address issues of a sensitive nature, and we have omitted that detailed information from this report. However, for the purposes of implementing the related recommendations that information was previously shared with ITD.

The response from the Comptroller of Maryland, on behalf of ITD, 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 Comptroller regarding the results of our review of its response.

# APPENDIX

COMPTROLLER of MARYLAND
Serving the People

**Peter Franchot**
*Comptroller*

**Sharonne R. Bonardi**
*Deputy Comptroller*

July 24, 2020

Mr. Gregory Hook, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, MD 21201

**RE: OLA Audit of Information Technology Division – Comptroller of Maryland**

Dear Mr. Hook:

Enclosed, please find the Information Technology Division's (ITD) responses to the legislative audit by your office conducted between June 4, 2014 through March 11, 2019.

As an agency entrusted with the custody of the sensitive information and data for millions of taxpayers, there is nothing that is more important to Comptroller Franchot and our team than the integrity and safety of taxpayer data. Over the past several years, we've taken several key measures to bolster our ability to safeguard taxpayer information.

Because of the Comptroller of Maryland's efforts to combat tax fraud, I have the honor of serving as the co-chair of the Senior Executive Board for the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center ("ISAC"), a position that provides an opportunity for our agency to share our best practices with members of the IRS' Security Summit. The Comptroller's Office has also worked successfully to align Risk Management and Information Technology activities to better identify, assess, and mitigate threats to the confidentiality, integrity, and availability of the agency's systems and the confidential data that the taxpayers of Maryland entrust to us. We have strengthened security and background checks for all employees and contractors. We have updated or replaced hundreds of outdated applications, databases, and servers with modern, highly secure systems. We have continued to improve our threat and incident detection and response capabilities. We have done all of these and more, while strengthening our ability to deliver first-class service to Maryland taxpayers.

We appreciate the value of third-party audits such as these as we constantly aspire to further improve our best practices. However, we do have respectful but strong points of disagreement over Finding 4. We do not concur with the Recommendation in Finding 4 and we appreciate the opportunity to discuss this in detail in our official response. We do, however, concur and have begun the process of implementing the remainder of the recommendations outlined in the findings.

As you are aware, the Comptroller’s Office is in the process of phasing in our new, state-of-the-art tax processing system that will build upon our record of efficiency and success. The ongoing, phased implementation of the COMPASS system will further transform our ability to protect taxpayers from cybercrime in this highly dangerous environment using automation, advanced analytics, and continuous monitoring that meet and exceed Federal and State security control requirements.

On behalf of Comptroller Franchot, thank you once again for your team’s diligent audit and for the opportunity to respond to the findings.

Sincerely,

Bonardi

Sharonne R. Bonardi
Deputy Comptroller

**Comptroller of Maryland**
**Information Technology Division**
**Annapolis Data Center Operations**

**Agency Response Form**

## Sensitive Personally Identifiable Information (PII)

| |
|---|
| **Finding 1**<br>**The Information Technology Division (ITD) maintained sensitive PII in a manner that did not provide adequate safeguards.** |

**We recommend that ITD implement appropriate information security safeguards for sensitive PII it maintains.**

| **Agency Response** | | | |
|---|---|---|---|
| **Analysis** | | | |
| **Please provide additional comments as deemed necessary.** | While data can be viewed by authorized users, data at rest includes hardware-based protections. | | |
| **Recommendation 1** | Agree | **Estimated Completion Date:** | |
| **Please provide details of corrective action or explain disagreement.** | There are additional products concerning this security issue that could be implemented. However, these additional more comprehensive mitigating controls will adversely impact day-to-day operations, require addressing the needs of 60+ unique agencies, and require funding unavailable at this time. In addition, the specific system reviewed is a legacy system that is in the process of being replaced. | | |

**Auditor's Comment**: ITD agreed with the recommendation but noted it would create adverse operational impact, affect multiple agencies, and require funding which was unavailable. On funding, ITD did not provide any related cost estimates. ITD also stated that the specific system reviewed was being replaced, whereas the finding cited that specific system as an example among multiple mainframe systems which processed sensitive PII information without use of adequate safeguards. Further, ITD's response was focused on just one of two options, per the finding analysis, for providing needed information security safeguards.

OLA' s position is that the PII should be adequately protected, as public studies have concluded that the cost of data breaches involving PII can be considerable, and potentially exceed the costs of preventive safeguards. We also believe that if remediation costs via a preferred security option are proven to be excessive, that ITD needs to pursue an alternate option, in a prioritized manner, to implement the three-part substantial mitigating controls, as defined per the *Information Technology Security Manual*, with related communications shared to customer agencies as necessary. Collectively, we believe that our finding is justified and the recommended action is both prudent and appropriate.

## Mainframe Software

**Finding 2**
**Controls involving access and monitoring over mainframe security software as well as database software reporting controls were not adequate.**

**We recommend that ITD**

**a. restrict access to critical operating and system software files to only those individuals requiring such access and log all such accesses (repeat);**

**b. ensure that the review of security software violation logs includes activity for all time periods and for all users (repeat); and**

**c. implement activity reporting for changes made to critical database management software catalog tables, review such reports for propriety, document these reviews, and retain the reviews for future reference.**

| Agency Response | | | |
|---|---|---|---|
| **Analysis** | | | |
| **Please provide additional comments as deemed necessary.** | Since the preliminary report we performed a comprehensive review, implemented additional restrictions, and conducted process improvements to improve access and monitoring over mainframe security. | | |
| **Recommendation 2a** | Agree | **Estimated Completion Date:** | 3Q 2020 |
| **Please provide details of corrective action or explain disagreement.** | Access has been restricted to the current extent possible to meet this recommendation. Of the 14 bulleted items:<br>1. 5 were completed<br>2. 1 was not completed (access deemed 'necessary')<br>3. 8 were partially completed with each of the 8 retaining access for a very small subset of # USERIDs. This access will remain until the level of access required changes<br><br>We are revamping our library naming conventions to keep in line with industry standards and simplify the identification of critical system libraries | | |

**Comptroller of Maryland**
**Information Technology Division**
**Annapolis Data Center Operations**

## Agency Response Form

| | | | |
|---|---|---|---|
| **Recommendation 2b** | Agree | **Estimated Completion Date:** | 4Q 2020 |
| **Please provide details of corrective action or explain disagreement.** | We are designing a new implementation approach for control and logging of all updates to critical system. This includes a regular review of such changes for certain critical types of libraries. | | |

| | | | |
|---|---|---|---|
| **Recommendation 2c** | Agree | **Estimated Completion Date:** | Completed |
| **Please provide details of corrective action or explain disagreement.** | Reporting is in place for the database software catalog table. Daily reviews and documentations of these reports is done by the mainframe security team. Results are permanently stored. | | |

## Network Security

**Finding 3**
**Network-based intrusion detection and prevention system (IDPS) coverage did not exist for traffic flowing into the ITD network from certain origin points, and the Comptroller of Maryland's mobile computers did not utilize a host-based firewall.**

**We recommend that ITD**

**a. ensure that IDPS protection exists for all traffic from untrusted sources entering the ITD network flowing to critical servers and network segments within the data center, and**

**b. work in conjunction with the Comptroller of Maryland's various divisions and units to ensure that all Comptroller laptop computers are protected by an enabled and properly configured host-based firewall.**

| **Agency Response** | | | |
|---|---|---|---|
| **Analysis** | | | |
| **Please provide additional comments as deemed necessary.** | No comment. | | |
| **Recommendation 3a** | Agree | **Estimated Completion Date:** | |
| **Please provide details of corrective action or explain disagreement.** | ITD agrees to implement IDPS protection for all traffic from untrusted sources and will investigate additional protection for internal neutral segments to determine if a cost beneficial solution can be implemented to enhance existing controls. | | |

## Agency Response Form

| | | | |
|---|---|---|---|
| **Recommendation 3b** | Agree | **Estimated Completion Date:** | End of 3Q 2020 |
| **Please provide details of corrective action or explain disagreement.** | We agree with this finding. Review of the options with our current suite of products is complete and we are developing our final recommendation for internal approval. This will be a large complex project and due to the risk involved when dealing with changes in production environments extensive planning and testing will occur prior to any implementation. | | |

**Finding 4**
**Security risks existed from information technology (IT) contractors having unnecessary network-level access to the Comptroller's network.**

**We recommend that ITD restrict IT contractors' network-level access within the Comptroller network to only those servers and workstations necessary for them to perform their duties (repeat).**

| **Agency Response** | | | |
|---|---|---|---|
| **Analysis** | | | |
| **Please provide additional comments as deemed necessary.** | This response is regarding full-time, contractor employees. Temporary contractors, such as vendor-provided project support, are treated differently. They are not granted unsupervised access, do not have system login or remote access accounts, and are not provided Comptroller equipment. All work performed is supervised onsite or through a remote screen-sharing mechanism. | | |
| **Recommendation 4** | Disagree | **Estimated Completion Date:** | |
| **Please provide details of corrective action or explain disagreement.** | The Comptroller of Maryland fully supports the principle of least privileged access, and enhancements to security controls within the environment.<br>Although this is a repeat finding, at present this recommendation still exceeds current State DoIT security policy, and Federal security requirements and guidance. The National Institute of Standards and Technology in September of 2019 released the first initial DRAFT of guidance for implementation of a zero-trust architecture (that would meet the recommendation by OLA) and, as of today, has not finalized the NIST 800-207 document. This recommendation is also not included in the current Cyber Security Framework for Critical Infrastructure maintained by the US Department of Homeland Security. | | |

| | |
|---|---|
| | Absent final guidance from the experts, agreement with this finding would place the Comptroller of Maryland in a position of having mandated controls that far exceed established requirements and control frameworks.<br><br>In addition, we would note that we have multiple compensating controls throughout the environment and prior to granting access, all contractors supporting the Comptroller of Maryland are subject to the same onboarding process as regular employees. This includes background investigations, fingerprinting, and orientation with the Office of Human Resources. Contractors also use Comptroller issued hardware and software that is maintained and secured by ITD. In addition, no employee, whether contractor or regular employee, has access to the entire network, whether direct hardwire, wireless or VPN. Access is controlled by various security mechanisms using the 'least privileged' concept to ensure access is granted only where required. |

**Auditor's Comment:** ITD disagreed with the recommendation to restrict IT contractors' network level access, by citing demonstrably incorrect information, which could mislead the reader. For example, the criteria cited by OLA in the Analysis in support of the principle of least privileged access, in fact, does not exceed the current State DoIT Security Policy, but is the current policy. The State of Maryland's IT security policy guidance has long required limiting access to IT resources as per the least privilege principle, both historically and per the current *Information Technology Security Manual* (ITSM). Our position that the State of Maryland's ITSM least privilege security principle extends to network security is long-standing and accepted by other State agencies, and as such requires restricting the Comptroller's IT contractors' network level access to only IT resources needing to be accessed to fulfill their contractual requirements.

Consequently, in our opinion, ITD is not in compliance with current State security policy and is placing its IT resources at risk by allowing its IT contractors unnecessary network-level access to almost all of the Comptroller's network (versus the Comptroller's described "entire network"). Finally, this a repeat finding, and in response to our prior report item, ITD agreed that contractors' network-level access should be restricted to only those servers and workstations to which each contractor requires access, a position that it now opposes without justification.

## AUDIT TEAM

**Richard L. Carter, CISA**
**R. Brendan Coffey, CPA, CISA**
Information Systems Audit Managers

**Edward O. Kendall, CISA**
**Edwin L. Paul, CPA, CISA**
Information Systems Senior Auditors

**Peter W. Chong**
**Joseph R. Clayton**
Information Systems Staff Auditors