DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

April 27, 2022

Senator Guy J. Guzzone, Chair
Senate Budget and Taxation Committee
Miller Senate Office Building, 3 West Wing
11 Bladen Street
Annapolis, Maryland 21401

Delegate Benjamin S. Barnes, Chair
House Appropriations Committee
Lowe House Office Building, Room 151
6 Bladen Street
Annapolis, Maryland 21401

Senator Clarence K. Lam, M.D., Senate Chair
Joint Audit and Evaluation Committee
Miller Senate Office Building, Room 420
11 Bladen Street
Annapolis, Maryland 21401

Delegate Carol L. Krimm, House Chair
Joint Audit and Evaluation Committee
Lowe House Office Building, Room 422
6 Bladen Street
Annapolis, Maryland 21401

Ladies and Gentlemen:

The Office of Legislative Audits (OLA) has reviewed the actions taken by the Comptroller of Maryland's Revenue Administration Division (RAD) and Information Technology Division (ITD), University System of Maryland - Frostburg State University (FSU), and the Baltimore County Public Schools

(BCPS) to resolve the repeat cybersecurity findings in our respective 2020 audit reports. This review was conducted in accordance with a requirement contained in the April 2021 *Joint Chairmen's Report* (JCR), pages 255 and 256.

The JCR required that, prior to the release of $100,000 of each agencies' administrative appropriation for fiscal year 2022, RAD, ITD, and FSU must have met with the State Chief Information Security Officer (SCISO) concerning their repeat cybersecurity findings. Furthermore, the meeting was to identify and document a path for resolution of any outstanding issues and to confirm that the agencies have taken corrective action with respect to their cybersecurity audit findings, including articulating any ongoing associated costs and a timeline for resolution if the corrective action is not complete. In addition, the JCR required the SCISO to submit a report to OLA by February 1, 2022 addressing corrective actions taken to remediate these cybersecurity audit findings, a path and timeline for resolution of any outstanding issues, and any ongoing costs associated with corrective actions. The JCR language further provided that OLA submit a report by May 1, 2022 to the budget committees and the Joint Audit and Evaluation Committee listing each repeat audit finding, along with information that demonstrates the agencies' commitment to correct each repeat audit finding. The JCR also stated that it was the intent of the General Assembly that the Baltimore County local school system should also complete the aforementioned process based on having had several repeat cybersecurity audit findings in its calendar 2020 compliance audit report.

In accordance with the April 2021 JCR requirement, the SCISO provided a report, dated January 3, 2022, detailing the corrective actions that RAD and ITD had taken with respect to the repeat audit findings. The SCISO provided a report addendum, dated February 18, 2022, detailing the corrective actions that FSU and BCPS had taken with respect to the repeat audit findings. Both the original January 3, 2022 report and the February 18, 2022 addendum can be found in Exhibit 1. The SCISO status report indicated that RAD, ITD, and FSU had taken corrective actions to address their respective repeat cybersecurity findings. The SCISO status report indicated that BCPS had taken corrective actions to address one of its three repeat cybersecurity findings, and, was making "meaningful" progress to address the two remaining repeat cybersecurity findings. Regarding FSU's and BCPS' status, the SCISO's report addendum contained some extraneous information and detailed sensitive information that OLA deemed necessary to redact from publication in this letter.

We reviewed the SCISO status report and related documentation and held discussions with the SCISO as necessary to assess the implementation status of the related recommendations. Based on our review of the actions described in the reports, it is our opinion that Finding 6 from the RAD report, Findings 2 and 4 from the ITD report, Finding 3 from the FSU report, and Finding 8 from the BCPS report related to cybersecurity have been resolved. In addition, we found that the actions taken by BCPS regarding the repeat audit report condition in Finding 9 (that is, recommendation 9a), in fact indicated the repeat finding had been satisfactorily resolved rather than BCPS making "meaningful" progress, since the SCISO report stated the servers involved in the finding were now protected in a security zone (a DMZ). Finally, we agree that BCPS has made progress and the remedial actions described in the status report demonstrated a commitment to correct repeat cybersecurity Finding 6 from "its calendar 2020 compliance audit report" (Exhibit 2 includes a summary of our review's conclusions).

We advised RAD, ITD, FSU, and BCPS of the results of our review. We wish to acknowledge the cooperation extended by RAD, ITD, FSU, BCPS, and the SCISO during this review and their willingness to address the cybersecurity audit issues and implement appropriate corrective actions.

We trust our response satisfactorily addresses the JCR requirement. Please contact me if you need additional information.

Sincerely,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

cc: Joint Audit and Evaluation Committee Members and Staff
Senator William C. Ferguson IV, President of the Senate
Delegate Adrienne A. Jones, Speaker of the House of Delegates
Governor Lawrence J. Hogan, Jr.

Comptroller Peter V.R. Franchot
Treasurer Dereck E. Davis
Attorney General Brian E. Frosh
Honorable David R. Brinkley, Secretary, Department of Budget and Management
John Hiter, Director, Information Technology Division, Comptroller of Maryland
Wayne P. Green, Director, Revenue Administration Division, Comptroller of Maryland
Mohammed Choudhury, State Superintendent of Schools, Maryland State Department of Education
Jay A. Perman, M.D., Chancellor, University System of Maryland
Linda R. Gooden, Chair, Board of Regents, University System of Maryland
Ronald H. Nowaczyk, Ph.D., President, Frostburg State University
Robert L. Page, Associate Vice Chancellor, Financial Affairs, University System of Maryland
David Mosca, Director, Office of Internal Audit, University System of Maryland
Julie C. Henn, Chair, Baltimore County Board of Education
Darryl L. Williams, Ed.D., Superintendent, Baltimore County Public Schools
Charles I. Stewart IV, State Chief Information Security Officer, Department of Information Technology
Victoria L. Gruber, Executive Director, Department of Legislative Services
Morgan T. Smith, Policy Analyst, Department of Legislative Services
Sara J. Baker, Policy Analyst, Department of Legislative Services
Hiram L. Burch, Manager, Policy Analyst, Department of Legislative Services

Exhibit 1 to April 27, 2022 Letter to Joint Chairmen and Joint Audit And Evaluation Committee

Maryland | DEPARTMENT OF INFORMATION TECHNOLOGY

January 3, 2022

The Honorable Sen. Guy Gazzone
Chair, Senate Budget and Taxation Committee
3 West, Miller Senate Building
Annapolis, Maryland 21401

The Honorable Delegate Maggie McIntosh
Chair, House Appropriations Committee
121 House Office Building
Annapolis, MD 21401

Dear Chairman and Madam Chair:

I respectfully submit the information requested in the 2021 Joint Chairmen's Report regarding the Review of State Cybersecurity on pages 57-58 and Agencies with Cybersecurity Audit Findings in 2020 on page 255. While referenced separately in the Joint Chairmen's Report, there is a high degree of interdependence between these items. For that reason, this document includes the response for both items separately.

If you have any questions, please do not hesitate to contact me.

Best regards,

Charles (Chip) Stewart
State Chief Information Security Officer
Department of Information Technology

Maryland | DEPARTMENT OF INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

Review of State Cybersecurity and Report on Agencies with Cybersecurity Audit Findings in 2020

Maryland Department of Information Technology

Office of Security Management

Completed pursuant to requirement described in the 2021 Joint Chairmen's Report, Pages 57-58

(State of Cybersecurity)

Due – November 19, 2021

Amended Due Date – January 3, 2022

Completed pursuant to requirement described in the 2021 Joint Chairmen's Report, Pages 255-256

(Agencies with Cybersecurity Audit Findings in 2020)

Due – February 1, 2022

January 3, 2022

Introduction

Over the past several years, Maryland has emerged as the cybersecurity capital of the United States. This advancement has been bolstered by an ongoing investment targeting cybersecurity improvements within the State, continued investment in the workforce, and supporting the growth of thousands of cybersecurity and technology companies in the State. Through these investments, Maryland has made significant progress in reducing cybersecurity risk and improving our ability to serve citizens with technology.

This report addresses the requirements described in the 2021 Joint Chairmen's Report, both for the "State of Cybersecurity" and "Agencies with Cybersecurity Audit Findings in 2020." While referenced separately in the Joint Chairmen's Report, there is a high degree of interdependence between these items. For that reason, this document includes the response for both items separately.

Structurally, the document begins with the supporting requests from the 2021 Joint Chairmen's Report. Following that section is the report describing cybersecurity in the State that includes the requirements of the Joint Chairmen's Report and generalized findings and actions taken based on the cybersecurity study initiated by the Maryland Cybersecurity Council. Finally, the document includes a review of all cybersecurity findings impacting units of State government, with a detailed evaluation of the repeat findings and efforts to address them.

The nature and content of the responses creates an opportunity to combine these reports, creating a more comprehensive response that more thoroughly answers both. The Department of Information Technology considers the exercises driven by these requests to be valuable in improving cybersecurity across the State and is happy to answer follow-up questions related to the information contained within these reports.

Report 2 – Report on Agencies with Cybersecurity Audit Findings in 2020

Section 47 Report on Agencies with Cybersecurity Audit Findings in 2020

SECTION 47. AND BE IT FURTHER ENACTED, That since three agencies have had repeat findings for cybersecurity in the calendar 2020 compliance audit reports issued by the Office of Legislative Audits (OLA), $100,000 of each of the general fund appropriations made for the purpose of administration in Program E00A04.01 Revenue Administration and Program E00A10.02 Information Technology Division in the Office of the Comptroller and $100,000 of the general fund appropriation for administration in Program R30B26.07 University System of Maryland – Frostburg State University, may not be expended until:

1. representatives from each identified entity with repeat cybersecurity audit findings in calendar 2020 have met with the State Chief Information Security Officer (SCISO) to identify and document a path for resolution of any outstanding issues, and the agency has taken corrective action with respect to cybersecurity audit findings, including articulating any ongoing associated costs and a timeline for resolution if the corrective action is not complete;
2. SCISO submits a report to OLA by February 1, 2022, addressing corrective actions taken to remediate cybersecurity audit findings, a path and timeline for resolution of any outstanding issues, and any ongoing costs associated with corrective actions; and
3. a report is submitted to the budget committees and the Joint Audit and Evaluation Committee by OLA, no later than May 1, 2022, listing each repeat audit finding in accordance with (1) above that demonstrates the agencies' commitment to correct each repeat audit finding.

Further provided that it is the intent of the General Assembly that the Baltimore County local school system, having had several repeat audit findings in the calendar 2020 compliance audit reports for cybersecurity, shall also be required to complete items (1), (2), and (3) of this section.

Further provided that the budget committees shall have 45 days from the date of receipt of the report to review and comment. Funds restricted pending the receipt of the report may not be transferred by budget amendment or otherwise and shall revert to the General Fund if the report is not submitted.

Information Request	Authors	Due Date
Report on repeat PII findings	SCISO	February 1, 2022
	OLA	May 1, 2022

Detailed Finding Information

Comptroller

Revenue Administration Division: Finding 6

Security and audit events for several critical databases were either not logged or not reviewed for propriety.

Analysis

For three critical systems, database security and audit events were either not logged or not reviewed for propriety.

- Logging was not enabled for seven user accounts which had the capability to process direct changes to one system's critical database tables. Also, a security system software report listed instances when direct changes were made to critical database tables such as those involving certain tax information, however, associated detail reporting of related specific change activity did not exist for use, to confirm that the direct changes made to critical tables were proper. A similar condition was commented upon in our two preceding audit reports concerning detailed change reports control weaknesses.
- One system's database security reports of grants and revokes of users' privileges and the assignment of changes to a userid were not reviewed for propriety. A similar condition was commented upon in our preceding audit report.
- Two systems' database security and audit events such as adding and configuring roles of system users and turning off the audit function were not logged even though the capability to perform such logging existed. A similar condition was commented upon in our two preceding audit reports.

These conditions could result in unauthorized or inappropriate activities (affecting the integrity of the production databases' information) going undetected by management.

The State of Maryland Information Technology Security Manual requires that information systems must generate audit records for all security-relevant events, and procedures must be developed to routinely (for example real time or weekly) review audit records for indications of inappropriate activities and report findings to appropriate officials for prompt resolution.

Detailed sensitive aspects of this finding were omitted from this report, however the related detailed information was previously shared with RAD for purposes of implementing the following recommendations.

Recommendation

We recommend that RAD implement appropriate database monitoring controls over the aforementioned critical tax systems. Specifically, we recommend that RAD:

a. ensure that logging is enabled for all user accounts granted database table level change capabilities;

b. ensure that reviews of the propriety of the critical security system software reports include a review of recently developed detail change reports (repeat);
c. log all critical database security and audit events (repeat); and
d. review all significant database security reports for propriety on a timely basis, document these reviews and retain the reviews for future reference.

Unit actions since the delivery of the audit report

The Comptroller's Chief Information Security Officer reports that all items associated with this finding have been reviewed and addressed. Additionally, the protection, logging, and monitoring of updates to system critical libraries has been expanded to an even wider set of system assets.

Costs associated with remediation

There was no additional cost associated with remediating this finding.

State Chief Information Security Officer Recommendation

Based on the information provided by the agency, the State Chief Information Security Officer believes that the Comptroller's office has resolved this issue.

Information Technology Division: 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

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.

Unit actions since the delivery of the audit report

The Comptroller's CISO reports that security violations and other substantive changes are being logged and reviewed as suggested in the recommendations, with a substantially increased log retention period. Additionally, access to critical operating system software files is restricted to those with a critical need.

The Comptroller's team also indicated ongoing activities in support of eliminating all "non-cancellable" ID's except in very controlled situations.

Costs associated with remediation

There was no additional cost associated with remediating this finding.

State Chief Information Security Officer Recommendation

Based on the information provided by the agency, the State Chief Information Security Officer believes that the Comptroller's office has resolved this issue.

Information Technology Division: Finding 4

Security risks existed from information technology 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

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).

Unit actions since the delivery of the audit report

On February 8, 2021, a meeting between the Comptroller's Team, the State Chief Information Security Officer, and the Office of Legislative Audits occurred to discuss this finding. The outcome of this meeting, shared as a memo to the chairs of the Joint Audit and Evaluation committee on March 5, 2021, describes the collective agreement of the three parties related to this finding. In summary, the three parties agreed that the more stringent personnel screening procedures and the system-level access controls results in no additional risk for contractors than for employees.

Costs associated with remediation

There were no costs associated with resolving this finding.

State Chief Information Security Officer Recommendation

Based on the outcome of the meeting and memo provided to the Joint Audit and Evaluation Committee, the State Chief Information Security Officer considers this finding to have been retracted.

Maryland DEPARTMENT OF INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

Addendum to the Review of State Cybersecurity and Report on Agencies with Cybersecurity Audit Findings in 2020

Maryland Department of Information Technology

Office of Security Management

Completed pursuant to requirement described in the 2021 Joint Chairmen's Report, Pages 57-58

(State of Cybersecurity)

Due – November 19, 2021

Amended Due Date – January 3, 2022

Completed pursuant to requirement described in the 2021 Joint Chairmen's Report, Pages 255-256

(Agencies with Cybersecurity Audit Findings in 2020)

Due – February 1, 2022

Amended Due Date – March 1, 2022

February 18, 2022

The SCISO's Addendum contained extraneous information and detailed sensitive information that OLA redacted from inclusion in this public document.

Addendum to Report 2 - Report on Agencies with Cybersecurity Audit Findings in 2020

Overview of Findings

The Office of Legislative Audits noted the following cybersecurity findings in the reports published in CY2020, listed alphabetically by the name used in the report. Following the overview, a detailed reporting from each agency with repeat findings is provided. Each of these items describes the finding, along with the status and SCISO review.

Baltimore County Public Schools

Information Technology Division (11/19/2020)

- **REPEAT** – BCPS did not ensure that employee access to its automated financial systems was appropriate and adequately controlled, resulting in employees with unnecessary or incompatible access.

[redacted]

- **REPEAT** – For two critical systems' databases, security and audit event logging and monitoring procedures were not adequate, and unnecessary elevated system privileges were granted to numerous user accounts.
- **REPEAT** – [redacted] publicly accessible servers were improperly located within the internal network, intrusion detection prevention system coverage for untrusted traffic did not exist, and BCPS network resources were not secured against improper access from students using wireless connections and high school computer labs.

Note: On November 24, 2020, Baltimore County Public Schools experienced a cyber attack against their computer network where ransomware was deployed. As a result of this incident, significant technological transformation occurred. This transformation resulted in many of the findings from the audit being resolved. As a result, no cost information is available regarding these items. Additional information from Baltimore County Public Schools is available at:

https://go.boarddocs.com/mabe/bcps/Board.nsf/files/CBJL85554478/$file/OLA%20Follow-up%20Results%20-%20AC%20Meeting.pdf

University System of Maryland

Frostburg State University (8/5/2020)

- **REPEAT** – FSU did not ensure that user access capabilities on its financial management systems were adequately restricted resulting in employees with unnecessary or inappropriate system capabilities.

Detailed Finding Information

Baltimore County Public Schools

Information Technology Division: Finding 6

BCPS did not ensure that employee access to its automated financial systems was appropriate and adequately controlled, resulting in employees with unnecessary or incompatible access.

Analysis

BCPS did not ensure employee access to its automated financial-related systems (such as, procurement, account payable, human resources, and payroll) was appropriate and adequately controlled, resulting in employees with unnecessary or incompatible access. BCPS maintains several automated systems to process critical financial activity that have the capability for online controls. Our review disclosed that BCPS did not use these controls to adequately limit user access, resulting in the following conditions:

- Our test of certain critical procurement and accounts payable access capabilities assigned to 68 employees disclosed 8 employees had the ability to process purchase orders without independent approval. Two of these employees could also process disbursements, and one could also update vendor information. Three other employees could process disbursements without independent approval.
- Our test of certain critical access capabilities for the automated system primarily used to order supplies for schools disclosed that 315 employees could initiate and approve requisitions without independent approval. These requisitions automatically generated purchase orders to the vendor without any additional independent review or approvals. During the period from May 10, 2017 through June 18, 2019, 128 employees initiated and approved requisitions for 3,203 purchase orders totaling approximately $1.1 million without any independent review and approval. A similar condition was commented upon in our preceding audit report.
- Our test of certain critical human resource and payroll access capabilities assigned to 209 employees disclosed that 5 employees who processed payroll transactions also had unnecessary access to human resources functions, (such as adding employees). Additionally, 2 other employees had incompatible human resource and payroll functions even though they did not require system access to perform their job responsibilities. A similar condition regarding incompatible system access to human resources and payroll capabilities has been commented upon in our two preceding audit reports.

Recommendation

We recommend that BCPS

a. periodically review employee access capabilities to ensure all access is appropriate and incompatible duties are segregated (repeat); and
b. correct any unnecessary or improper capabilities, including those noted above.

Unit actions since the delivery of the audit report

- The provision of an employee's system access report for management's review was suspended due to the cyber-attack. Reporting to management is anticipated to resume by the fall of 2022.

- Changes were made to the access of the identified employees.
- The automated ordering system, ESchoolMall, referenced in OLA's audit report was replaced with an internally hosted site effective January 2021.

Outstanding Matters:

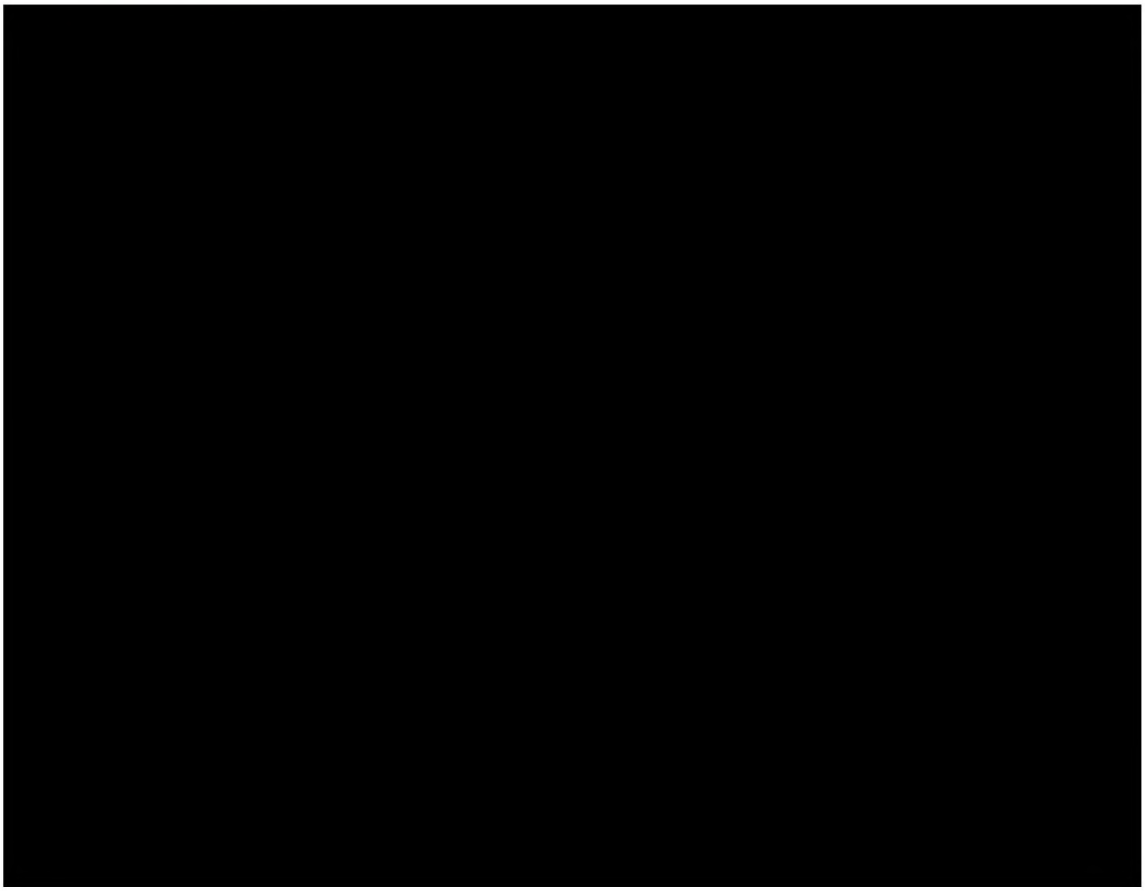
- The system access report for management's use is not available until FY23.
- A SOP has not been implemented regarding the reporting of employees' system access to management.

Costs associated with remediation

There is no cost information provided for the resolution of this item.

State Chief Information Security Officer Recommendation

Based on the information provided by BCPS, the SCISO believes that BCPS is making meaningful progress in resolving this finding.



[redacted]

Information Technology Division: Finding 8

For two critical systems' databases, security and audit event logging and monitoring procedures were not adequate, and unnecessary elevated system privileges were granted to numerous user accounts.

Analysis

For two critical systems' databases, security and audit event logging and monitoring procedures were not adequate, and unnecessary elevated system privileges were granted to numerous user accounts.

- One system's database configuration did not include logging of eight categories of critical security and audit related events. For such activity already recorded, we were advised that the associated logs were not retained for adequate time periods, and that reviews of the logs were not performed on a regular basis to identify unusual or improper activities. The second critical system's database configuration also did not include logging of the same eight categories of critical security and audit related events. Furthermore, although BCPS personnel advised us that reviews of other significant logged database events were performed, BCPS was unable to provide documentation substantiating the performance of these reviews.
- Neither of the systems' databases were configured to log direct changes (such as insert, update, and delete) made to critical system tables for subsequent reporting and monitoring. Accordingly, effective monitoring did not exist over sensitive activities related to these systems and their related databases.
- Numerous user accounts had unnecessary modification access to the information within both systems' databases. For both systems, improper database roles were assigned to 34 user accounts, effectively granting the highest possible administrative privilege level available to these accounts over the respective databases.

These conditions could result in unauthorized or inappropriate activities (affecting the integrity of the production databases' information) going undetected by management. Best practices identified in the State of Maryland Information Technology Security Manual require that information systems must generate audit records for all security-relevant events, and procedures must be developed to routinely (for example, real-time or weekly) review audit records for indications of inappropriate activities and report findings to appropriate officials for prompt resolution. Similar conditions regard controls for logging critical systems' security and audit event activity and direct changes to database information were commented upon in our preceding audit report. A similar condition regarding assigned database roles, for one of the two systems' databases, was also commented upon in our preceding audit report.

Detailed sensitive aspects of this finding were omitted from this report; however, the related detailed information was previously shared with BCPS for purposes of implementing the following recommendations.

Recommendation

We recommend that BCPS implement appropriate database monitoring controls over the aforementioned critical systems. Specifically, we recommend that BCPS

a. log all significant database security, audit related event, and processing activities, including direct changes to critical database tables, and generate reports that include this related database activity (repeat);
b. ensure that individuals perform regular, independent documented reviews of the aforementioned reports and retain the information for reference purposes (repeat); and
c. restrict assignment of critical database administration roles to only those personnel requiring such access for their job responsibilities (repeat).

Unit actions since the delivery of the audit report

As previously described, due to the cyber-attack, BCPS migrated this function to cloud-based systems. BCPS staff do not have server-level access to these systems as they are hosted by the respective software vendors.

Costs associated with remediation

There is no cost information provided for the resolution of this item.

State Chief Information Security Officer Recommendation

Based on the transformation that BCPS describes following their cybersecurity incident, the SCISO believes that the BCPS team has resolved these findings.

Information Technology Division: Finding 9

[redacted] **publicly accessible servers were improperly located within the internal network, intrusion detection prevention system coverage for untrusted traffic did not exist, and BCPS network resources were not secured against improper access from students using wireless connections and high school computer labs.**

Analysis

The BCPS computer network was not adequately secured. We noted three conditions affecting network security.

- [redacted] publicly accessible servers were located within the BCPS internal network rather than being isolated in a separate protected network zone to minimize security risks. These publicly accessible servers, if compromised, could expose the internal network to attack from external sources. Recommended security procedures, as stated in the National Institute of Standards and

Technology Guidelines on Firewalls and Firewall Policy, include placing publicly accessible servers in an external protected zone to protect those servers, as well as the entity's internal network. A similar condition was commented upon in our preceding audit report.

- Intrusion detection prevention system (IDPS) coverage did not exist for untrusted encrypted traffic entering the BCPS network. BCPS operated a network appliance having integrated IDPS; however, the appliance was configured to only analyze unencrypted traffic. Additionally, server host-based intrusion prevention system coverage was not utilized for this untrusted encrypted traffic. We identified 21 firewall rules that allowed encrypted traffic from any source to 29 unique network destinations within BCPS' internal network without IDPS coverage. The aforementioned absence of IDPS coverage creates network security risk as such traffic could contain undetected malicious data. Best practices in the State of Maryland Information Technology Security Manual require protection against malicious code and attacks by using IDPS to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.
- BCPS did not adequately secure its critical internal network resources from improper network-level access by BCPS students using wireless connections and high school students using computer lab workstations. Wireless network access existed for BCPS students within the various schools locations; however, BCPS did not use adequate network-level traffic filtering to properly limit such access. Additionally, within BCPS' 24 high schools, the network traffic originating from students using computer labs' workstations was not filtered to control such access. Accordingly, per the aforementioned wireless and computer labs access, students were allowed unnecessary network-level access to administrative servers within both BCPS' data center and the individual schools locations. Student BCPS network access via wireless connections and from high schools computer labs should be limited via filters to devices and ports necessary for these students to perform required educational tasks. Best practices in the State of Maryland Information Security Policy require that entities' networks must ensure that only authorized individuals have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of least possible privilege and need to know.

Recommendation

We recommend that BCPS

a. relocate all publicly accessible servers to a separate protected network zone to limit security exposures to the internal network segment (repeat);
b. perform a documented review and assessment of its network security risks and identify how IDPS coverage should be applied to its network for all untrusted traffic, including encrypted traffic, and implement this coverage; and
c. limit student network-level access from wireless connections and high school computer labs to only authorized local school and system instructional network resources.

Unit actions since the delivery of the audit report

BCPS has migrated to a "largely cloud based SaaS model" that has eliminated "the vast majority of public facing servers." Additionally, publicly accessible servers that could expose the network to attack from outside sources are no longer in use:

- the [redacted] servers identified in the prior audit were encrypted and are now protected in the BCPS DMZ.
- the DMZ provides an additional layer of security to BCPS' local area network and limits access from external sources.
- new firewall rules were implemented and student access to the entire data center was removed.

Costs associated with remediation

There is no cost information provided for the resolution of this item.

State Chief Information Security Officer Recommendation

Based on the information provided by BCPS, the SCISO believes that BCPS is making meaningful progress in resolving this finding.

University System of Maryland

Frostburg State University: Finding 3

FSU did not ensure that user access capabilities on its financial management systems were adequately restricted resulting in employees with unnecessary or inappropriate system capabilities.

Analysis

FSU did not ensure that user access capabilities on its financial management systems were adequately restricted to prevent improper transactions. Although reports of user access granted to each FSU employee were provided to management personnel for their review, these reviews did not identify all unnecessary or inappropriate system access. Furthermore, these reviews were performed only on an annual basis. We reviewed system capabilities assigned to 313 users for nine critical functions related to each of the following areas: student financial aid, student accounts, payroll, and procurements and disbursements.

- Fifteen system users were assigned access to critical student financial aid capabilities even though they did not need the access for their assigned jobs. In addition, 7 users (including 2 of the aforementioned 15) had access to process critical transactions without independent approval. Specifically, all 7 could modify student financial data used to determine student eligibility for federal aid and 5 of the 7 could also create and modify student financial aid budgets that establish a maximum amount of aid a student can receive.
- One user had excessive access to student accounts including the ability to adjust student accounts without any independent approval and process related cash receipts. Subsequent to our inquiries, the access to adjust student accounts was removed because the user did not need it for their assigned job.

Similar conditions regarding unnecessary or inappropriate system access were commented upon in our preceding audit report. USM's IT Security Standards specify that institutions must segregate critical functions to ensure the appropriate separation of duties for system users. In addition, institutions are responsible for ensuring that access rights reflect employee status, including changes in employee status.

Recommendation

We recommend that FSU ensure that user access capabilities in its financial management systems are adequately restricted to prevent improper transactions. Specifically, we recommend that FSU

a. use its annual review of user access capabilities to ensure that system access to perform critical functions is restricted to those employees who require such access for their job duties, and in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions (repeat);
b. consider conducting reviews of user access capabilities on a more frequent basis than annually; and
c. address the unnecessary and inappropriate access identified in our finding.

Unit actions since the delivery of the audit report

In response to the recommendations of a Legislative Audit Report, Frostburg State University (FSU) has been working to address the three parts of the report's recommendations ("a." – "c.") as it relates to restricting access to specific financial aid management system processes. Specifically, FSU has followed up to ensure that user access capabilities in its financial aid management systems are adequately restricted to prevent improper transactions. This is accomplished by:

- conducting an annual review of user access capabilities to ensure that system access to perform critical functions is restricted to those employees who require such access for their job duties, and in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions;
- addressing unnecessary and inappropriate access identified in the finding; and
- the implementation of a new [redacted] cloud-based financial aid software system.

Page 8 of the Legislative Audit report noted that fifteen system users were assigned access to critical student financial aid capabilities even though they did not need the access for their assigned jobs. In addition, the report found that 7 users (including 2 of the aforementioned 15) had access to critical transactions without independent approval. Specially all 7 could modify student financial aid data used to determine student eligibility for financial aid and 5 of the 7 could also create and modify student financial aid budgets that establish a maximum amount of aid a student can receive.

In response, in spring of 2021, FSU removed access from 11 of the 15 people to the Admissions Applications Basis of Admission report [redacted] which contains student financial aid information, and corrected 3 to view access only, and left 1 in update status.

In response to the recommendation that the student financial aid data and the Free Application for Federal Student Aid (FAFSA) verification status be modified/changed, a trigger was added to the page(s) and a trace file was generated using a random 1% selection of the changes which has been reported to the Assistant Vice President for Finance and Budget and the Assistant to the President, weekly.

Subsequent to the steps taken by FSU to respond to the OLA report, as is standard procedure, USM Internal Audit conducted a follow up review and determined the following as it relates to the three OLA report recommendations:

Status a: Implemented

USM Internal Audit reviewed and confirmed that FSU used its annual review of user access capabilities to ensure that system access to perform critical functions is restricted to those employees who require such access for their job duties, and in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions.

Status b: Implemented

USM Internal Audit reviewed and confirmed that FSU agreed to conduct reviews of user access capabilities on a more frequent basis than annually. FSU now performs semi-annual reviews. USM Internal Audit verified that FSU conducted the Fall 2020 and Spring 2021 semi-annual reviews.

Status c: Not Fully Implemented

USM Internal Audit reviewed and confirmed that FSU partially addressed the unnecessary and inappropriate access noted by the OLA report, which was for student financial aid access.

FSU explained that due to the small staff size of the financial aid office, they cannot reduce the number of SFA staff with computer access. Instead, FSU was implementing a compensating control procedure to allow current financial aid staff to perform their duties but have an independent employee review all transactions when users modify student financial data and create and modify student financial aid budgets.

In addition, USM Internal Audit also found three Admissions department employees that still had inappropriate access identified by OLA's report.

The OLA recommendation "c." was to be considered implemented by USM Internal Audit when FSU:

- Completed implementation of the compensating control procedure mentioned above. FSU was to verify that this new procedure ensures a proper segregation of duties and independent review and approval of critical transactions.
- Removed the student financial aid access to the three Admissions department employees with inappropriate access identified by OLA's report (this has been completed).

FSU full implementation of OLA Recommendation "c."

During fall of 2021, FSU began implementation a new [redacted] software solution: Student Financial Planning (SFP). SFP is a trigger-based cloud system in place for 2022-2023 (this new software system is now in production at FSU). This software (being implemented by several USM institutions) represents a significant investment on the part of FSU. It improves efficiency, productivity, and the user experience. Its functionality also addresses the remaining outstanding recommendation ("c.") in the OLA report. Specifically, the need for a compensating control procedure to allow current financial aid staff to perform their duties but have an independent employee review all transactions when users modify student financial data and create and modify student financial aid budgets. Given its functionality, and that SFP is now in production at FSU, this recommendation is now considered met by FSU. USM has provided evidence describing how the new functionality meets the letter and spirit of the OLA recommendations.

Implementation of SFP has eliminated the need for FSU to use a trigger generated trace file to randomly generate a 1% selection of changes made to the Free Application for Federal Student Aid (FAFSA) verification status of students currently reported to the Assistant Vice President for Finance and Budget and the Assistant to the President, weekly for independent verification.

Separation of duties will be adhered to throughout SFP via various security roles. FSU will continue to provide Owners of Data Reports every 6 months to be reviewed to confirm compliance for separation of duties.

Costs associated with remediation

Because resolution of recommendation "c" occurred as part of a planned project, there was no additional cost associated with remediating this finding. There were no costs associated with resolution of recommendation "a" or "b" beyond baseline.

State Chief Information Security Officer Recommendation

Based on the information provided by the Internal Audit Team and the Chief Information Officer of the University System of Maryland, the State Chief Information Security Officer believes that this finding has been appropriately resolved.

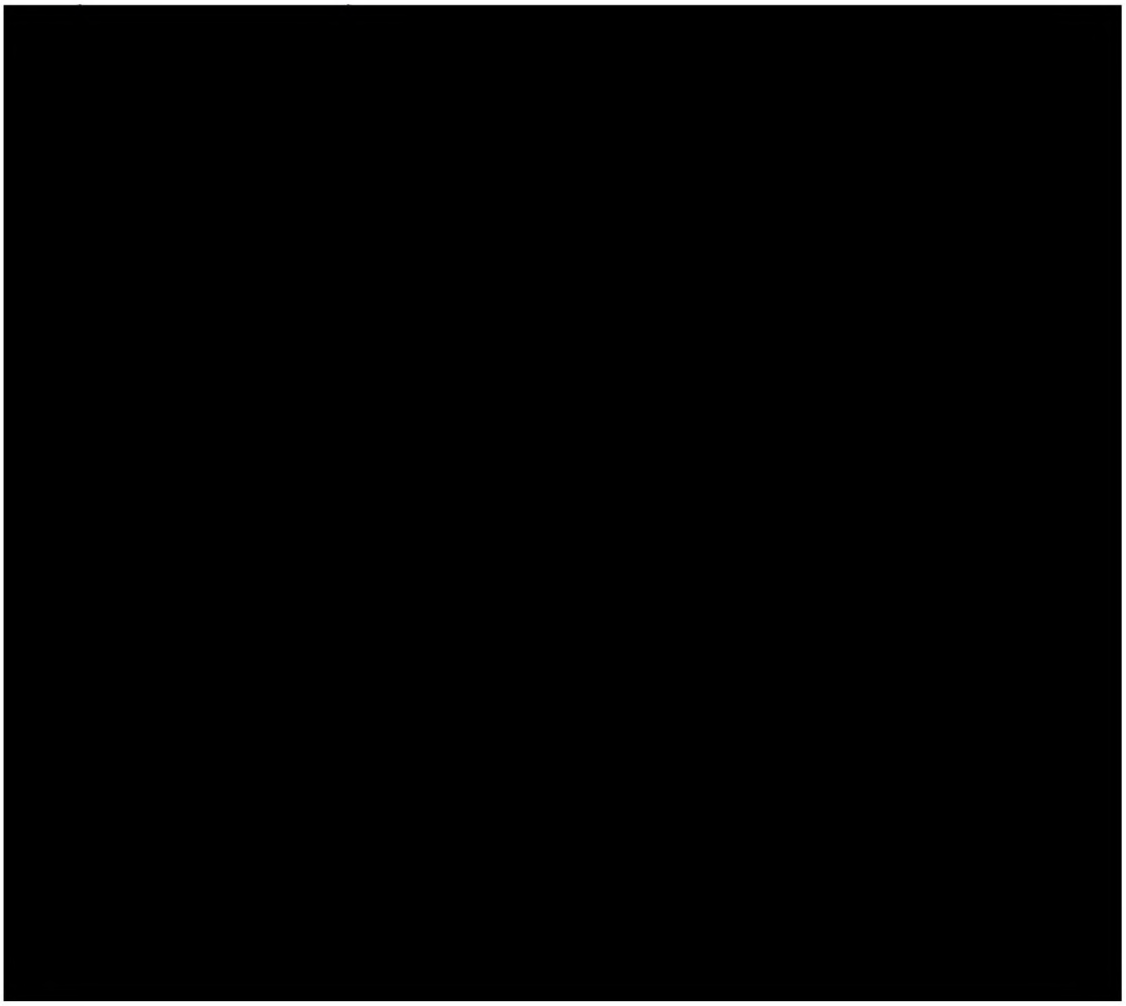


Exhibit 2
Status of Repeat Cybersecurity Findings in OLA's 2020 Audit Reports of the Comptroller of Maryland's Revenue Administration Division and Information Technology Division, University System of Maryland – Frostburg State University, and the Baltimore County Public Schools

Prior Recommendations Pertaining to Repeat Findings	Status Based on OLA Review
Revenue Administration Division Finding 6 – We recommend that RAD implement appropriate database monitoring controls over the aforementioned critical tax systems. Specifically, we recommend that RAD b. ensure that reviews of the propriety of the critical security systems software reports include a review of recently developed detail change reports (repeat)	Resolved
c. log all critical database security and audit events (repeat)	Resolved
Information Technology Division Finding 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)	Resolved
b. ensure that the review of security software violation logs includes activity for all time periods and for all users (repeat)	Resolved
Finding 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)	Resolved
Frostburg State University Finding 3 – We recommend that FSU ensure that user access capabilities in its financial management systems are adequately restricted to prevent improper transactions. Specifically, we recommend that FSU	Resolved

a. use its annual review of user access capabilities to ensure that system access to perform critical functions is restricted to those employees who require such access for their job duties, and in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions (repeat)	
Baltimore County Public Schools Finding 6 – We recommend that BCPS a. periodically review employee access capabilities to ensure all access is appropriate and incompatible duties are segregated (repeat)	In Progress
Finding 8 – We recommend that BCPS implement appropriate database monitoring controls over the aforementioned critical systems. Specifically, we recommend that BCPS a. log all significant database security, audit related event, and processing activities, included direct changes to critical database tables, and generate reports that include this related database activity (repeat)	Resolved
b. ensure that individuals perform regular, independent documented reviews of the aforementioned reports and retain the information for reference purposes (repeat)	Resolved
c. restrict assignment of critical database administration roles to only those personnel requiring such access for their job responsibilities (repeat)	Resolved
Finding 9 – We recommend that BCPS a. relocate all publicly accessible servers to a separate protected network zone to limit security exposures to the internal network segment (repeat)	Resolved