DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

April 14, 2021

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

Delegate Maggie McIntosh, Chair
House Appropriations Committee
House Office Building, Room 121
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
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 Department of Budget and Management (DBM), Office of the State Treasurer (STO), and Maryland State Department of Education (MSDE) to resolve the repeat personally identifiable information (PII) findings in our respective 2019 audit reports. This review was conducted in accordance with a requirement contained in the April 2020 *Joint Chairmen's Report* (JCR), pages 245 and 246.

The JCR required that, prior to the release of $100,000 of each agencies' administrative appropriation for fiscal year 2021, DBM, STO, and MSDE must have met with the State Chief Information Security Officer (SCISO) concerning their repeat PII finding. 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 PII protection, 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, 2021 addressing corrective actions taken to protect PII, 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, 2021 to the budget committees and the Joint Audit and Evaluation Committee (JAEC) listing each repeat audit finding along with information that demonstrates the agencies' commitment to correct each repeat audit finding.

In accordance with the April 2020 requirement, the SCISO provided a report to OLA, dated January 26, 2021, detailing the corrective actions that DBM, STO, and MSDE had taken with respect to the repeat audit findings (Exhibit 1). The SCISO status report indicated that DBM and STO had taken corrective actions to address their respective repeat PII findings. The SCISO status report indicated that MSDE is making progress to address its repeat PII finding. Regarding MSDE's status, the SCISO's status report contained detailed sensitive information about current remediation efforts 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 report, it is our opinion that the DBM and STO PII audit report findings (Finding 10 and Finding 5, respectively) have been resolved. In addition, we found that MSDE was making progress and the remedial actions described in the status report demonstrated a commitment to correct PII audit report Finding 4 (Exhibit 2). Due to the redaction of certain sensitive material and OLA not describing the MSDE corrective actions in a public document, we hope that the aforementioned OLA opinion on MSDE's actions will be sufficient for the purposes of this letter.

We advised DBM, STO, and MSDE of the results of our review. We wish to acknowledge the cooperation extended by DBM, STO, MSDE, and the SCISO

during this review and their willingness to address the 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, 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 Nancy K. Kopp
Attorney General Brian E. Frosh
Honorable David R. Brinkley, Secretary, Department of Budget and Management
Karen B. Salmon, Ph.D., State Superintendent of Schools
Charles I. (Chip) Stewart IV, State Chief Information Security Officer, Department of Information Technology
Victoria L. Gruber, Executive Director, Department of Legislative Services
Anne P. Wagner, Policy Analyst, Department of Legislative Services
Samuel M. Quist, Policy Analyst, Department of Legislative Services
Laura H. Hyde, Policy Analyst, Department of Legislative Services

Exhibit 1 to April 14, 2021 Letter to Joint Chairmen and Joint Audit and Evaluation Committee

Maryland DEPARTMENT OF INFORMATION TECHNOLOGY

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

Report on Agencies with Multiple Personally Identifiable Information Audit Findings in 2019

Maryland Department of Information Technology

Office of Security Management

Completed pursuant to requirement described in the 2020 Joint Chairmen's Report, Pages 245-246

January 26, 2021

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

Report Requirement

SECTION 42. AND BE IT FURTHER ENACTED, That since three agencies have had repeat findings in the calendar 2019 compliance audit reports issued by the Office of Legislative Audits (OLA) for problems protecting personally identifiable information (PII), $100,000 of the general fund appropriation for administration in Program E20B01.01 Treasury Management in the State Treasurer's Office, $100,000 of the general fund appropriation for administration in Program F10A01.01 Executive Direction in the Department of Budget and Management Office of the Secretary, and $100,000 of the general fund appropriation for administration in Program R00A01.01 Office of the State Superintendent in the State Department of Education Headquarters may not be expended until:

(1) agency representatives from agencies with repeat PII audit findings in calendar 2019 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 PII protection, including articulating any ongoing associated costs and a timeline for resolution if the corrective action is not complete;
(2) the SCISO submits a report to OLA by February 1, 2021 addressing corrective actions taken to protect PII, 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 (JAEC) by OLA listing each repeat audit finding in accordance with above that demonstrates the agencies' commitment to correct each repeat audit finding. The report shall be submitted to the budget committees and JAEC by May 1, 2021, and the committees and JAEC shall have 45 days to review and comment from the date the report is submitted. 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.

Explanation: Commonly accepted cybersecurity standards are guided by CIA, which stands for confidentiality, integrity, and availability. Protecting PII is a key element of confidentiality. Not all State agencies are properly protecting PII. Audit reports from calendar 2019 identified repeat PII findings in the Department of Budget and Management, State Department of Education, and Office of the State Treasurer. This language requires that these agencies report their plans to correct outstanding PII issues to the SCISO. The SCISO should review these plans and report to OLA about these agencies' plans. OLA should review SCISO's findings and report on the commitment to resolving these repeat findings to the budget committees and JAEC.

Information Request	**Authors**	**Due Date**
Report on repeat PII findings	SCISO	February 1, 2021
	OLA	May 1, 2021

Maryland DEPARTMENT OF INFORMATION TECHNOLOGY

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

Mr. Hook,

Safeguarding sensitive information, including Personal Information (PI)/Personally Identifiable Information (PII), hereafter referred to as PII, is imperative to the Maryland Department of Information Technology. Maryland law mandates the protection of this information, and federal law and regulation require the same in many cases. The Department of Information Technology is committed to collaborating with agencies to protect the sensitive information that the public trusts us to guard. The challenges in protecting this information include many technical and administrative issues that we will address through this response.

An ongoing challenge faced by many organizations, including units of the State government, is understanding the data lifecycle, including understanding the requirements for retention and eventual destruction. DoIT considers there to be two categories of sensitive information described in the OLA audit reports. It is imperative to bifurcate these two categories for the findings because they require varying remediations. Further details are outlined below:

1. The first category is information that agencies must retain, but auditors identified inadequate safeguards for its storage.
2. The second category of information is that which is no longer required, but the agencies failed to purge from its systems.

Data described by the first category must be protected as described in Maryland State Government Code §10–1304. Because of the complex circumstances in each of these findings, there is no universal solution to ensure appropriate protections. The Office of Security management has worked collaboratively with each of the identified units to ensure implementation of adequate safeguards and supplemental protections, when applicable.

The second category of sensitive information is that which is still stored, with no requirement for retention. In these cases, it is the goal of the SCISO to ensure the appropriate disposal of these records by taking reasonable steps and considerations as described in Maryland State Government Code §10–1303. In most cases, the activities required to resolve the repeat findings associated with information that has reached the end of its retention period was simply the purging of the data.

DoIT appreciates the hard work and collaboration with the agencies that has resulted in substantive progress in resolving and addressing the initial audit findings.

Thank you,

Charles "Chip" Stewart
State Chief Information Security Officer

Department of Budget and Management

Financial Management Information System

Information Systems Security and Control

Finding 10 (Repeat)

Sensitive PII maintained by CCU was stored without adequate safeguards.

Analysis

Sensitive PII maintained by CCU was stored without adequate safeguards (see Finding 2 for comment on user access to PII). Specifically, we reviewed one application and determined that as of May 2018, one file within CCU's debt collection application contained 1,216,224 unique SSNs stored in clear text along with associated names and addresses. In addition, we were advised that this sensitive PII was not protected by other substantial mitigating controls. This PII is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. A similar condition was commented upon in our preceding audit report. The State of Maryland Information Technology Security Manual requires that confidential data should be protected using encryption and/or other substantial mitigating controls.

Recommendation 10

We recommend that DBM use approved encryption methods or other substantial mitigating controls to properly protect all sensitive PII (repeat).

Unit actions since the delivery of the audit report

DoIT verified with DBM that, after the audit but before the audit report was released, DBM implemented a new debt management collection system to replace the legacy RPCS System. According to DBM staff, their team implemented the new debt management collection system "***Debt Manager***" in July of 2019. In contrast with the inadequate protection that the previous system provided, the new system provides adequate protection of stored Personal Information/Personally Identifiable Information by encrypting data at rest. The legacy system has since been retired from service.

Costs associated with remediation

Because remediation occurred by replacing an outdated system before issuance of this report, there is no expectation that the unit will incur additional costs.

State Chief Information Security Officer Recommendation

The SCISO believes that, by replacing the legacy system with a new system, the unit has met its obligation by resolving this audit finding and recommends releasing the restriction on fund expenditures.

State Treasurers Office

Information Systems Security and Control

Finding 5 (Repeat)

Sensitive personally identifiable information (PII) maintained by STO was stored without adequate safeguards.

Analysis

Sensitive PII maintained by STO was stored without adequate safeguards. Specifically, as of July 2018, we identified two files residing on a critical server which contained 157,090 and 117,916 unique social security numbers in clear text, with related full names. In addition, we determined that this sensitive PII was not protected by other substantial mitigating controls. STO had initiated a project for conversion of the aforementioned critical server, which included encrypting the PII upon being transferred to a new server, but as of August 2018 the project had not been completed. This sensitive PII, which is commonly associated with identity theft, should be protected by appropriate information system security controls. The State of Maryland Information Security Policy states that agencies should protect confidential data using encryption technologies and/or other substantial mitigating controls. A similar condition was commented upon in our preceding audit report.

Recommendation 5

We recommend that STO properly protect the aforementioned sensitive PII by the use of encryption or other substantial mitigating controls (repeat).

Unit actions since the delivery of the audit report

Before delivery of the report, in December of 2018, STO made updates to remediate the findings, including removal of unnecessary PII and encryption of sensitive information when in transit. This action fully addressed the recommendation described in the finding.

Starting in July of 2020, Treasury has worked to deploy DoIT provided tools to scan their environment for unencrypted PII contained within files. Since deploying these tools, the Treasurer's office IT staff has removed most unprotected sensitive data.

The Treasurer's office IT staff has also implemented an administrative control requiring their staff to check the monitoring system, at least monthly, for improperly stored sensitive information.

While unexpected delays impacted the migration timeline, the STO expects the project to be completed by the end of FY2021.

Costs associated with remediation

Because remediation occurred by initiating a project to replace the outdated system before issuance of this report, there is no expectation that the unit will incur additional costs.

State Chief Information Security Officer Recommendation

The SCISO believes that, with the changes made to the legacy system and its imminent replacement with a new system, the unit has met its obligation by resolving this audit finding and recommends releasing the restriction on fund expenditures.

Maryland State Department of Education (MSDE)

Information Systems Security and Control

Finding 4 (Repeat)

Sensitive personally identifiable information (PII) maintained by MSDE was stored without adequate safeguards.

Analysis

Sensitive PII maintained by MSDE was stored without adequate safeguards. Specifically, we obtained confirmation from MSDE management personnel that certain significant applications included databases in which PII was stored in clear text. For example, as of June 29, 2018, we determined that separate databases for statewide student and teacher identity information held 1,430,940 unique student names and Social Security numbers (SSNs) and 233,130 unique teacher names and SSNs, respectively; all stored in clear text. In addition, we noted that this sensitive PII was not adequately protected by other substantial mitigating controls such as the use of data loss prevention software. Furthermore, while MSDE had manually inventoried its applications as of September 2017 to identify all sensitive PII, we determined that this effort was incomplete and had not included the identification of PII in all MSDE applications, including those noted above with PII stored in clear text. A similar condition concerning PII storage was commented upon in our preceding audit report. This sensitive PII is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. The State of Maryland Information Security Policy states that confidential data should be protected using encryption and/or other substantial mitigating controls.

Recommendation 4

We recommend that MSDE, in conjunction with DoIT,

a. perform a manual inventory of all of its systems, identify all sensitive PII, and delete all unnecessary sensitive PII; and
b. use an approved encryption method, or other substantial mitigating controls to properly protect all necessary sensitive PII (repeat).

Unit actions since the delivery of the audit report

MSDE leadership initiated an effort to complete its 2021 data and systems inventory, including systems that may collect or contain PII and reports an expectation to have the inventory update finalized by 2/15/2021. This activity has already led to the decommissioning of several PII-containing systems that were no longer required, resulting in a cost-saving and reduced risk.

To address the second recommendation by OLA, DoIT began scanning MSDE's servers and workstations for unencrypted PII in files beginning in 2019. Through a collaborative effort, MSDE staff removed much of the unencrypted PII that was stored without adequate safeguards. The items that remain fall into three categories:

1. Transactional user data stored on workstations and user's home directories containing their own PII (e.g., HR Documents)

The SCISO's Status Report contained detailed sensitive information about current remediation efforts that OLA redacted from inclusion in this public document.

2. Data that is temporarily stored by the system during ingestion
3. Data, stored in databases and other data structures, that are not encrypted when not in-use

[redacted]

State Chief Information Security Officer Recommendation

The SCISO believes that, while still in progress, MSDE has undertaken substantive efforts to rectify the findings and made a good-faith effort to meet their projected timelines. While the unit missed these deadlines, the totality of the circumstance yields a recommendation to release the restriction on fund expenditures.

Exhibit 2
Status of Repeat PII Findings in OLA's 2019 Audit Reports of the Department of Budget and Management, the Office of the State Treasurer, and the Maryland State Department of Education

Prior Recommendations Pertaining to Repeat Findings	Status Based on OLA Review
Department of Budget and Management Finding 10 – We recommend that DBM use approved encryption methods or other substantial mitigating controls to properly protect all sensitive PII (repeat).	Resolved
Office of the State Treasurer Finding 5 – We recommend that STO properly protect the aforementioned sensitive PII by the use of encryption or other substantial mitigating controls (repeat).	Resolved
Maryland State Department of Education Finding 4 – We recommend that MSDE, in conjunction with DoIT, a. perform a manual inventory of all of its systems, identify all sensitive PII, and delete all unnecessary PII; and	In Progress
b. use an approved encryption method, or other substantial mitigating controls to properly protect all necessary sensitive PII (repeat).	In Progress