Audit Report

Financial Management Information System
Centralized Operations

November 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

November 10, 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 conducted a fiscal compliance audit pertaining to information system security and operational controls over the centralized operations of the Financial Management Information System (FMIS) as administered by the Department of Information Technology (DolT) and the Comptroller of Maryland's General Accounting Division (GAD). FMIS is used to support the State's purchasing, accounting, and payment functions. According to the State's accounting records, expenditures processed through FMIS for fiscal year 2019 totaled approximately $47 billion.

Our audit disclosed that DoIT's procedures for logging and monitoring critical database and mainframe security events were not sufficient.

DoIT's response to this audit is included as an appendix to this report. We reviewed the response to our finding and related recommendations, and have concluded that the corrective actions identified are sufficient to address all audit issues.

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

Respectfully submitted,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900 · Toll Free in Maryland 877-486-9964
Fraud Hotline 877-FRAUD-11 · www.ola.state.md.us

Background Information

General Information

The Financial Management Information System (FMIS) is an integrated database system that runs on the Comptroller of Maryland's Annapolis Data Center's computers and supports individual agency and Statewide purchasing and accounting operations. FMIS's purchasing and accounting components are operational in virtually all Executive Branch agencies, with the exception of the University System of Maryland (USM) and the Maryland Department of Transportation (MDOT). Because of unique requirements, USM and the Maryland Judiciary process procurement, disbursement, and financial information on in-house computer systems that interface certain financial information to FMIS for recordation, payment processing, and reporting. An additional interface entity is MDOT, which operates its own customized version of FMIS. With respect to interfaced data, our centralized audit included a review of the controls and processing of such data from the point of interface to FMIS through transaction processing and recordation.

According to the State's accounting records, expenditures processed through FMIS for fiscal year 2019 totaled approximately $47 billion; this includes the aforementioned State agencies that use their own computer systems that interface with FMIS.

Control Agency Responsibilities

FMIS supports purchasing functions through the Advanced Purchasing and Inventory Control System (ADPICS) component, and supports the accounting operations through the Relational Standard Accounting and Reporting System (R*STARS) component. The integration of procurement and accounting processing within FMIS results in two primary agencies, the Department of Information Technology (DoIT) and the Comptroller of Maryland, having responsibility for separate aspects of FMIS.

Specifically, DoIT is responsible for daily FMIS administration, including maintenance, operation, security, and back-up of related database records and the computer programs that perform online and overnight processing. The Comptroller of Maryland's General Accounting Division (GAD) is primarily responsible for R*STARS operations, security, and reporting.

DoIT and GAD are separately audited by the Office of Legislative Audits with respect to their agency-specific FMIS responsibilities. This audit of the

centralized FMIS operations included elements of FMIS operations relative to the State's overall internal control that are not included in the aforementioned agency audits, such as database and security controls. For an expanded explanation of the nature and purpose of this audit, see the Audit Scope, Objectives, and Methodology section of this report.

Findings and Recommendations

Finding 1
The Department of Information Technology's (DoIT's) procedures for logging and monitoring critical database and mainframe security events were not sufficient.

Analysis
DoIT's procedures for logging and monitoring critical database and mainframe security events were not sufficient.

- Within the Financial Management Information System (FMIS) production database, direct changes to critical tables by four employees were not logged. Also, direct changes to critical tables by other employees were logged, and according to DoIT personnel were reviewed; however, the named reviewer was not independent of the change process and these reviews were not documented. Additionally, logging occurred for certain other significant database security and audit events (for example, granting and revoking users' privileges) and, while DoIT personnel asserted that reviews were made of these events, DoIT could not provide documentation to support the review of 7 of 10 daily reports we tested. Accordingly, unauthorized and inappropriate changes to production data within the FMIS database could have occurred without detection by management.

- For the FMIS production mainframe system, security reporting or monitoring procedures were not adequate. As of June 2020, DoIT personnel advised us that significant logging activity reports were generated, but had not been reviewed since August 2018. These reports listed mainframe activity for modifications of significant data and programs files, and for additions, changes, and deletions of security software rules governing these same data and program files. Accordingly, DoIT lacked assurance as to the propriety of significant data and program files' modifications, and security software rules changes governing file access and mainframe transactions.

The State of Maryland *Information Technology Security Manual* requires that information systems must generate audit records for all security-relevant events, including all security and system administrator accesses and procedures must be developed to routinely (for example, daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution.

Recommendation 1
We recommend that DoIT implement the following actions and that all related documentation be retained for future reference. Specifically, DoIT should

a. **log direct changes to critical database tables by all employees with such access, generate reports of such changes and other database security and audit events, perform independent, timely, and documented reviews of these reports; and**
b. **generate reports of critical mainframe security events and transactions, and perform timely, documented reviews of these reports (including examination of supporting documentation).**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit pertaining to information system security and operational controls over the centralized operations of the Financial Management Information System (FMIS). Fieldwork associated with our audit was conducted during the period from April 2020 to July 2020. 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 finding and conclusions based on our audit objectives.

The integration of procurement and accounting processing within FMIS results in two primary agencies, the Department of Information Technology (DoIT) and the Comptroller of Maryland's General Accounting Division (GAD), having responsibility for separate aspects of FMIS. As FMIS is a vital procurement and accounting application in virtually all State agencies, internal control over FMIS is critical to these State agencies. Since we are responsible for auditing these agencies and evaluating their internal control, we periodically evaluate FMIS's internal control.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the elements of FMIS operations relative to the State's overall internal controls (for example, database and security controls) and to evaluate compliance with applicable State laws, rules, and regulations not included in our individual audits of DoIT and GAD.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included central FMIS security administration and maintenance, and the component operations of the Advanced Purchasing and Inventory Control System (ADPICS) and of the Relational Standard Accounting and Reporting System (R*STARS).

The Maryland Department of Transportation (MDOT) maintains its own version of FMIS, which is audited separately. In addition, certain State agencies—including the Judiciary, University System of Maryland, and MDOT—process procurement, disbursement, and financial information on in-house computer systems that interface certain financial information to centralized FMIS for recordation, payment processing, and reporting. With respect to interfaced data, our centralized audit included a review of the controls and processing of such data from the point of interface to FMIS through transaction processing and recordation.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, tests of transactions, and, to the extent practicable, observations of FMIS operations. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from FMIS. The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from this source were sufficiently reliable for the purposes the data were used during this audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

DoIT and GAD are responsible for establishing and maintaining effective internal control over FMIS operations. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records; effectiveness and efficiency of operations including safeguarding of assets; and compliance with applicable laws, rules, and regulations are achieved. 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 FMIS centralized operations, were considered by us during the course of the 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 a finding relating to a condition that we consider to be a significant deficiency in the design or operation of internal control that could adversely affect the State's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. This finding is also considered a significant instances of noncompliance with applicable laws, rules, or regulations.

DoIT's response to our finding 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 DoIT regarding the results of our review of its response.

APPENDIX

Maryland | DEPARTMENT OF INFORMATION TECHNOLOGY

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

November 5, 2020

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

Dear Mr. Hook:

The Department of Information Technology (DoIT) has received the fiscal compliance audit pertaining to information system security and operational controls over the centralized operations of the Financial Management Information System (FMIS) by the Department of Legislative Services, Office of Legislative Audits, dated October 2020.

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

Sincerely,

Michael G. Leahy
Michael G. Leahy (Nov 5, 2020 14:34 EST)

Michael G. Leahy
Secretary, Department of Information Technology

Financial Management Information System
Centralized Operations

Agency Response Form

Finding 1
The Department of Information Technology's (DoIT's) procedures for logging and monitoring critical database and mainframe security events were not sufficient.

We recommend that DoIT implement the following actions and that all related documentation be retained for future reference. Specifically, DoIT should

a. log direct changes to critical database tables by all employees with such access, generate reports of such changes and other database security and audit events, perform independent, timely, and documented reviews of these reports; and

b. generate reports of critical mainframe security events and transactions, and perform timely, documented reviews of these reports (including examination of supporting documentation).

Agency Response			
Analysis			
Please provide additional comments as deemed necessary.			
Recommendation 1a	Agree	**Estimated Completion Date:**	Completed
Please provide details of corrective action or explain disagreement.	**DoIT has implemented new processes that include logging direct changes to critical database tables and generating reports of such changes and other database security and audit events. All reports will be independently reviewed timely, documented and retained accordingly.**		
Recommendation 1b	Agree	**Estimated Completion Date:**	Completed
Please provide details of corrective action or explain disagreement.	**DoIT has implemented new processes that include generating reports of critical mainframe security events and transactions. All reports will be independently reviewed timely, documented and retained accordingly.**		

AUDIT TEAM

Robert A. Wells, Jr., CPA
Audit Manager

Edwin L. Paul, CPA, CISA
Information Systems Audit Manager

Julia M. King
Senior Auditor

Eric Alexander, CPA, CISA
Information Systems Senior Auditor