GEORGE MASON UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2021

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of George Mason University (University) as of and for the year ended June 30, 2021, and issued our report thereon, dated February 17, 2022. Our report, included in the University's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.gmu.edu. Our audit of the University for the year ended June 30, 2021, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

Our audit also included testing over the major federal programs of the Student Financial Assistance Programs Cluster and Education Stabilization Fund for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; and identified one internal control finding and instance of noncompliance requiring management's attention in relation to this testing, which we reported in our separately issued Student Financial Assistance Programs Cluster Report. We first identified and reported this finding, titled "Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act," during our fiscal year 2020 audit. Our current audit found the University has taken adequate corrective action with respect to this finding and recommendation.

-TABLE OF CONTENTS-

STATUS OF PRIOR YEAR FINDING AND RECOMMENDATION

Continue Improving Security Awareness Training
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020, with significant progress)
Prior Title: Improve Security Awareness Training

George Mason University (University) is not meeting certain requirements in the National Institute of Standards and Technology Standard, 800-53 (NIST Standard) for security awareness training (SAT). In general, the control weaknesses relate to ensuring all users complete SAT and to providing role-based training to certain users with specific privileged security roles and responsibilities. An established SAT program is essential to protecting agency information technology systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the University.

We communicated the details of the control weaknesses to the University in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to its sensitivity and description of security mechanisms.

The University should prioritize and dedicate the necessary resources to address the concerns communicated in the FOIAE document. The fiscal year 2022 audit will include an evaluation of the University's completed corrective action and determine whether the University satisfactorily resolved the weaknesses.

INTERNAL CONTROL AND COMPLIANCE FINDING AND RECOMMENDATION

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not implement some of the required controls to protect the database management system (database) that supports the student financial system of record. The University's adopted information security standard, the NIST Standard, and industry best practices, such as the Center for Internet Security's Oracle 19c Database Benchmark (CIS Benchmark), prescribe several required and recommended security controls to safeguard systems that contain or process sensitive data.

We identified three controls that the University does not implement that are generally related to access and baseline configuration management. We communicated these specific control weaknesses to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

By not meeting the minimum requirements in the CIS Benchmark and aligning the database's settings and configurations with industry best practices, the University cannot ensure data integrity within the database and may not be able to determine if malicious or fraudulent activity is occurring within the database. The University should address the risks present in the database and document exceptions, as necessary. Implementing these processes and controls will help maintain the confidentiality, integrity, and availability of university data and meet the requirements defined in the CIS Benchmark.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

February 17, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
George Mason University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **George Mason University** (University) as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated February 17, 2022. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of the University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Continue Improving Security Awareness Training" and "Improve Database Security," which are described in the sections titled "Status of Prior Year Finding and Recommendation" and "Internal Control and Compliance Finding and Recommendation," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Status of Prior Year Finding and Recommendation" and "Internal Control and Compliance Finding and Recommendation" in the findings titled "Continue Improving Security Awareness Training" and "Improve Database Security."

The University's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on February 17, 2022. The University's response to the findings identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Finding and Recommendation

The University has not taken adequate corrective action with respect to the previously reported finding titled "Improve Security Awareness Training." Accordingly, we included this finding in the section titled "Status of Prior Year Finding and Recommendation." The University has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks

GEORGE MASON UNIVERSITY

4400 University Drive, Fairfax, Virginia 22030
Phone: 703-993-1000

February 17, 2022

Staci Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2021 audit by the Auditor of Public Accounts (APA) and discussed during the exit conference.

George Mason University acknowledges and concurs with the audit findings. The following contains APA's findings and management's responses to the concerns and issues raised.

Continue Improving Security Awareness Training

George Mason University (University) is not meeting certain requirements in the National Institute of Standards and Technology Standard, 800-53 (NIST Standard) for security awareness training (SAT). In general, the control weaknesses relate to ensuring all users complete SAT and to providing role-based training to certain users with specific privileged security roles and responsibilities. An established SAT program is essential to protecting agency IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the University.

We communicated the details of the control weaknesses to the University in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to its sensitivity and description of security mechanisms.

The University should prioritize and dedicate the necessary resources to address the concerns communicated in the FOIAE document.

The fiscal year 2022 audit will include an evaluation of the University's completed corrective action and determine whether the University satisfactorily resolved the weaknesses.

Management's Response

The University concurs with the recommended additional controls described in the FOIA Exempt management letter. Corrective actions for the cited control deficiencies will be addressed in a timely manner as detailed in the corrective action plan.

Improve Database Security

The University does not implement some required controls to protect the database management system (database) that supports the student financial system of record. The University's adopted information security standard, the NIST Standard and industry best practices, such as the Center for Internet Security's Oracle 19c Database Benchmark (CIS Benchmark) prescribe several required and recommended security controls to safeguard systems that contain or process sensitive data.

We identified three controls that the University does not implement that are generally related to access and baseline configuration management. We communicated these specific control weaknesses to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

By not meeting the minimum requirements in the CIS Benchmark and aligning the database's settings and configurations with industry best practices, the University cannot ensure data integrity within the database and may not be able to determine if malicious or fraudulent activity is occurring within the database.

The University should address the risks present in the database and document exceptions as necessary. Implementing these processes and controls will help maintain the confidentiality, integrity, and availability of university data and meet the requirements defined in the CIS Benchmark.

Management's Response

The University concurs with the recommended additional controls described in the FOIA Exempt management letter. Corrective actions for the cited control deficiencies will be addressed in a timely manner as detailed in the corrective action plan.

Sincerely,

Carol Dillon Kissal
Senior Vice President, Administration and Finance

GEORGE MASON UNIVERSITY

As of June 30, 2021

BOARD OF VISITORS

James W. Hazel, Rector

Horace Blackman, Vice Rector

Simmi Bhuller, Secretary

Anjan Chimaladinne
Thomas M. Davis
Juan Carlos Iturregui
Mehmood S. Kazmi
Wendy Marquez
Ignacia S. Moreno
Carolyn J. Moss
Jon M. Peterson
Nancy G. Prowitt
Paul J. Reagan
Edward H. Rice
Denise T. Roth
Bob Witeck

UNIVERSITY OFFICIALS

Gregory Washington, President

Carol D. Kissal, Senior Vice President for Administration and Finance

Deb Dickenson, Vice President of Finance

Sharon Heinle, Associate Vice President and Controller