GEORGE MASON UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, 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, 2019, and issued our report thereon, dated March 26, 2020. 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 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.

We did not perform audit work related to the prior audit finding entitled "Improve Compliance over Enrollment Reporting" because the University did not implement corrective action during our audit period. We will follow up on this finding during the fiscal year 2020 audit. The University took adequate corrective action with all of the remaining findings.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Develop and Implement a Process to Maintain Oversight over Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

George Mason University (University) is not gaining assurance that all information technology (IT) service providers (providers) have effective operating controls to protect the University's sensitive and confidential data. Providers are organizations that perform certain business tasks or functions on behalf of the University. The University has a process in place to assess and approve departments use of providers during contract negotiation and procurement, but does not have any formal processes to gain assurance on a regular basis that agreed upon security controls are in place and operating effectively. The University does not perform regular security audits of each provider's IT environment or consistently request and review independent audit reports, such as System and Organization Controls (SOC) reports, from each service provider.

The University requires all contracts with providers that may create, obtain, transmit, use, maintain, process, store, or dispose of sensitive University data to contain a data protection addendum wherein the provider agrees to adhere to certain security requirements. The addendum states that the University has the right to conduct audits of the provider at any time, and that the provider must conduct, or have conducted, an annual independent security audit that attests to the provider's security policies, procedures, and controls. The addendum further states that the provider must provide the results of independent security audits at the University's request, and that the provider must modify its security measures, based on the results of the audit, to meet the controls agreed upon in the addendum. The University's security standard, based on the National Institute of Standards and Technology Standard, 800-53 (NIST Standard), recognizes that organizations may procure IT equipment, systems, or services from third-party service providers and states that organizations must ensure that such providers meet the organization's established security requirements. Additionally, the NIST Standard requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis *(NIST Standard section: SA-9 External Information System Services)*.

By not defining and employing a process to gain assurance over providers' operating controls, the University cannot validate that the providers have effective IT controls to protect the University's sensitive and confidential data, increasing the chance of a breach or possible data disclosure. The University has a draft procedure that outlines the processes for gaining assurance over providers' operating controls and expects to approve and implement it in 2020.

The University should approve the draft processes they have to gain assurance providers have effective operating controls to protect the University's sensitive and confidential data on an ongoing basis. After the University approves the formal process for ongoing provider oversight, they should implement it into their information security program. By implementing a sufficient process to gain assurance over their providers, the University will help to ensure the confidentiality, integrity, and availability of sensitive data.

Improve Patch and Vulnerability Management

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not manage the wireless local area network controllers in accordance with University policy and its adopted information security standard, the NIST Standard.

We communicated two control weaknesses and compliance references to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The NIST Standard requires the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

In general, the weaknesses relate to the University not having certain patch management documentation and processes and not appropriately configuring a software tool it uses to help manage the controllers. Without the necessary procedures and appropriately configuring software tools, the University increases the risk that a malicious attacker will exploit an existing vulnerability that could lead to a data breach or affect system availability.

The University should ensure the documentation, processes, and tools it uses to manage the wireless local area network controllers align with University policy and the NIST Standard. By making these improvements, the University will reduce the risk to its sensitive and mission critical data

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

March 26, 2020

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, 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** as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated March 26, 2020. 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 to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

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 over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting 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 over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Develop and Implement a Process to Maintain Oversight over Service Providers" and "Improve Patch and Vulnerability Management," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," 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 determination of financial statement amounts. 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 section titled "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Develop and Implement a Process to Maintain Oversight over Service Providers" and "Improve Patch and Vulnerability Management."

George Mason University's Response to Findings

We discussed this report with management at an exit conference held on March 30, 2020. 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 Findings

We did not perform audit work related to the finding included in our report dated January 9, 2019, entitled "Improve Compliance over Enrollment Reporting" because the University did not implement corrective action during our audit period. We will follow up on this finding during the fiscal year 2020 audit. The University took adequate corrective action with all of the remaining findings.

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 Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks

GEORGE MASON UNIVERSITY
Senior Vice President
4400 University Drive, MS 3B2, Fairfax, Virginia 22030
Phone: 703-993-8750; Fax: 703-993-8772

April 1, 2020

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2019 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.

APA Finding – Develop and Implement a Process to Maintain Oversight over Service Providers

George Mason University (University) is not gaining assurance that all information technology (IT) service providers (providers) have effective operating controls to protect the University's sensitive and confidential data. Providers are organizations that perform certain business tasks or functions on behalf of the University. The University has a process in place to assess and approve departments use of providers during contract negotiation and procurement, but does not have any formal processes to gain assurance on a regular basis that agreed upon security controls are in place and operating effectively. The University does not perform regular security audits of each provider's IT environment or consistently request and review independent audit reports, such as System and Organization Controls (SOC) reports, from each service provider.

The University requires all contracts with providers that may create, obtain, transmit, use, maintain, process, store, or dispose of sensitive University data to contain a data protection addendum wherein the provider agrees to adhere to certain security requirements. The addendum states that the University has the right to conduct audits of the provider at any time, and that the provider must conduct, or have conducted, an annual independent security audit that attests to the provider's security policies, procedures, and controls. The addendum further states that the provider must provide the results of independent security audits at the University's request, and that the provider must modify its security measures, based on the results of the audit, to meet the controls agreed upon in the addendum. The University's security standard, based on the National Institute of Standards and Technology Standard, 800-53 (NIST Standard), recognizes that organizations may procure IT equipment, systems, or services

from third-party service providers and states that organizations must ensure that such providers meet the organization's established security requirements. Additionally, the NIST Standard requires that organizations define and employ processes to monitor security control compliance by external service providers on an ongoing basis *(NIST Standard section: SA-9 External Information System Services)*.

By not defining and employing a process to gain assurance over providers' operating controls, the University cannot validate that the providers have effective IT controls to protect the University's sensitive and confidential data, increasing the chance of a breach or possible data disclosure. The University has a draft procedure that outlines the processes for gaining assurance over providers' operating controls and expects to approve and implement it in 2020.

The University should approve the draft processes they have to gain assurance providers have effective operating controls to protect the University's sensitive and confidential data on an ongoing basis. After the University approves the formal process for ongoing provider oversight, they should implement it into their information security program. By implementing a sufficient process to gain assurance over their providers, the University will help to ensure the confidentiality, integrity, and availability of sensitive data.

Management's Response

As noted above, the university currently performs initial risk assessments of prospective service providers and has a draft process to provide ongoing assurance through annual SOC report reviews. The University's Information Technology Services unit will work with Purchasing, Finance, and other impacted units to refine, formalize, and implement a more comprehensive service provider risk management program by the end of December, 2020.

APA Finding - Improve Patch and Vulnerability Management

The University does not manage the wireless local area network controllers in accordance with University policy and its adopted information security standard, the NIST Standard.

We communicated two control weaknesses and compliance references to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The NIST Standard requires the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

In general, the weaknesses relate to the University not having certain patch management documentation and processes and not appropriately configuring a software tool it uses to help manage the controllers. Without the necessary procedures and appropriately configuring software tools, the University increases the risk that a malicious attacker will exploit an existing vulnerability that could lead to a data breach or affect system availability.

The University should ensure the documentation, processes, and tools it uses to manage the wireless local area network controllers align with University policy and the NIST Standard. By making these improvements, the University will reduce the risk to its sensitive and mission critical data.

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, 2019

BOARD OF VISITORS

Thomas M. Davis, Rector

James W. Hazel, Vice Rector

Shawn N. Purvis, Secretary

Karen Alcalde
Horace L. Blackman
Anjan Chimaladinne
Stephen M. Cumbie
Wendy Marquez
Ignacia S. Moreno
David Petersen
Nancy Gibson Prowitt
Paul J. Reagan
Edward H. Rice
Denise Turner Roth
Bob Witeck
Lisa Zuccari

UNIVERSITY OFFICIALS

Àngel Cabrera, President

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

Carol H. McGinnis, Interim Controller and Associate Controller