GEORGE MASON UNIVERSITY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2020

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, 2020, and issued our report thereon, dated March 31, 2021. 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, 2020, 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 Research and Development 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 found no internal control findings requiring management's attention or instances of noncompliance in relation to this testing.

-TABLE OF CONTENTS-

	Pages
AUDIT SUMMARY	
STATUS OF PRIOR YEAR FINDING AND RECOMMENDATION	1
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	2-4
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	5-7
UNIVERSITY RESPONSE	8-12
UNIVERSITY OFFICIALS	13

STATUS OF PRIOR YEAR FINDING AND RECOMMENDATION

Report Accurate and Timely Enrollment Data to the National Student Loan Data System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Compliance over Enrollment Reporting

During aid year 2020, University personnel implemented procedures which resulted in partial correction of the prior year finding. Based on our procedures, the University has resolved errors resulting in accurate and timely data being reported to the National Student Loan Data System (NSLDS) for students graduating from the University. However, University personnel did not report accurate and/or timely student status change data to the NSLDS for students that had withdrawn. The underlying cause of the errors is related to the need for University personnel to evaluate leave of absence and withdrawal policies, which resulted in students being inaccurately reported as being in a "Leave of Absence" or "Less than Half-Time" enrollment status in the NSLDS. From a review of 50 students (25 graduates and 25 students that had withdrawn), we identified the following deficiencies:

- eight students (16%) have an incorrect effective enrollment status;
- the effective date for ten students (20%) is inaccurate; and
- four students (8%) tested were not certified timely.

In accordance with 34 CFR § 685.309 and further outlined in the NSLDS Enrollment Guide, published by the Department of Education, enrollment changes must be reported to the NSLDS within 30 days when attendance changes, unless a roster file will be submitted within 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Untimely and inaccurate data submission to the NSLDS can affect the reliance placed on the system by the Department of Education for monitoring purposes and other higher education institutions when making aid decisions. Noncompliance may also have implications on an institution's participation in Title IV programs and can potentially impact loan repayment grace periods.

Management should evaluate leave of absence and withdrawal policies and implement changes which improve the accuracy and timeliness of the NSLDS student enrollment status change submissions. Management should ensure that such policies align with federal requirements. Management should implement corrective action to prevent future noncompliance and should consider implementing a quality control review (QCR) process to monitor the accuracy of submitted enrollment batches at both the campus and program levels in the NSLDS.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Implement Third-Party Service Provider Oversight Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University developed and began implementing a service provider oversight process in December 2020 to gain annual assurance that all information technology (IT) service providers (providers) have effective operating controls to protect the University's critical and confidential data. However, the University has not yet requested and reviewed independent audit reports, such as System and Organization Controls (SOC) reports, or an acceptable substitute, from each provider across all hosted systems.

Specifically, the University has not obtained a SOC report or an acceptable substitute for four of the 21 providers hosting protected data classified as highly sensitive data (HSD). The University also has not obtained audit assurance from the 16 providers hosting protected data classified as restricted data. Additionally, the University has not completed documentation of control deficiencies, along with mitigating controls, for 17 of the 21 providers hosting protected data classified as HSD or for any of the 16 providers hosting protected data classified as restricted data.

The University's *Third-Party Risk Management Process* document requires that the University request and evaluate annual security assessment reports from providers, identify compliance gaps, develop mitigation plans, and escalate issues of non-compliance. The University's security standard, the National Institute of Standards and Technology Standard, 800-53 (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)*.

Due to resource restraints, the University determined to initially target completing the process for providers hosting protected data classified as highly sensitive data. By not fully implementing the process to gain assurance over all 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 should dedicate the necessary resources to complete its efforts to request and evaluate annual security assessment reports from each provider to ensure the provider has effective operating controls to protect the University's sensitive and confidential data. During the evaluation, the University should identify control deficiencies, develop mitigation plans, and escalate issues of non-compliance, as needed. By gaining assurance over each provider, the University will help to ensure the confidentiality, integrity, and availability of sensitive data.

Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University does not implement cybersecurity requirements of the Gramm-Leach-Bliley Act (GLBA) for some systems containing customer information in accordance with the Code of Federal Regulations and University policy. The University completed a System Security Plan (SSP) that identifies risks to the security, confidentiality, and integrity of customer information and assesses the safeguards in place to control these risks for two systems, including the financial system of record that stores student and financial data. However, the University has not evaluated each of their systems to determine what systems contain customer information. The University also has not completed a sensitive systems list and completed an SSP for each system on the sensitive systems list.

The Code of Federal Regulations, Part 314.4, requires that organizations develop, implement, and maintain the information security program to safeguard customer information and complete a risk assessment that includes consideration of risks in each relevant area of operation. The *Information Technology Security Program* policy requires that all employees, students, visitors, and contractors must comply with the *Information Technology Security Standard.* The *Information Technology Security Standard* requires that the University develop and maintain a SSP for each sensitive system that assesses the system environment and controls.

Without implementing cybersecurity requirements of the GLBA for each system containing customer information, the University may not be able to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The University completed its new *Information Technology Security Standard* in July 2019 after transitioning from ISO 27002 to the NIST 800-53 Security Standard. The University then began a plan to evaluate each of their systems to determine what systems contain customer information and complete an SSP for each system. However, due to resource constraints and project prioritization, the University has not yet conducted the risk evaluations and implemented the controls necessary to meet the cybersecurity requirements of the GLBA for each system containing customer information.

The University should evaluate their systems to determine what systems contain customer information, then document a sensitive systems list and complete an SSP for each system on the list. Doing this will protect the security, confidentiality, and integrity of customer information and meet the requirements set forth in the GLBA.

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

The University is not meeting certain requirements in the 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 information 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.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

March 31, 2021

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
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, 2020, 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 31, 2021. 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 opinion 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 entitled "Report Accurate and Timely Enrollment Data to the National Student Loan Data System," "Implement Third-Party Service Provider Oversight Process," "Implement Cybersecurity Requirements of the GLBA," and "Improve Security Awareness Training," which are described in the sections titled "Status of Prior Year Finding and Recommendation" and "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 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 Findings and Recommendations" in the findings and recommendations entitled "Report Accurate and Timely Enrollment Data to the National Student Loan Data System," "Implement Third-Party Service Provider Oversight Process," "Implement Cybersecurity Requirements of the GLBA" and "Improve Security Awareness Training."

The University's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on March 31, 2021. The University's response to the findings and recommendations 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 and Recommendations

The University has not taken adequate corrective action with respect to the previously reported findings and recommendations included in the section "Status of Prior Year Findings and Recommendations." The University has taken adequate corrective action with respect to audit findings and recommendations 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
Carol Dillon Kissal
Senior Vice President for Administration and Finance
4400 University Drive, MS 3B2, Fairfax, Virginia 22030
Phone: 703-993-8750

March 31, 2021

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 2020 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 – Report Accurate and Timely Enrollment Data to the National Student Loan Data System

During aid year 2020, we determined that University personnel had implemented procedures which resulted in partial correction of the prior year finding. The procedures appear to have resolved errors resulting in accurate and timely data being reported to the National Student Loan Data System (NSLDS) for students graduating from the University. However, University personnel did not report accurate and/or timely student status change data to the NSLDS for students that had withdrawn. The underlying cause of the errors is related to the need for University personnel to evaluate leave of absence and withdrawal policies, which resulted in students being inaccurately reported as being in a "Leave of Absence" or "Less than Half-Time" enrollment status in the NSLDS. From a review of 50 students (25 graduates and 25 students that had withdrawn), we identified the following deficiencies:

- Eight students (16%) have an incorrect effective enrollment status;
- The effective date for ten students (20%) is inaccurate; and
- Four students (8%) tested were not certified timely.

In accordance with Code of Federal Regulations 34 CFR § 685.309 and further outlined in the NSLDS Enrollment Guide, published by the Department of Education, enrollment changes must be reported to the NSLDS within 30 days when attendance changes, unless a roster file will be submitted within 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Untimely and inaccurate data submission to the NSLDS can

affect the reliance placed on the system by the Department of Education for monitoring purposes and other higher education institutions when making aid decisions. Noncompliance may also have implications on an institution's participation in Title IV programs and can potentially impact loan repayment grace periods.

Management should evaluate leave of absence and withdrawal policies and implement changes which improve the accuracy and timeliness of the NSLDS student enrollment status change submissions. Management should ensure that such policies align with federal requirements. Management should implement corrective action to prevent future noncompliance and should consider implementing a quality control review (QCR) process to monitor the accuracy of submitted enrollment batches at both the campus and program levels in the NSLDS.

Management's Response

Based on our review, there are two separate issues that contributed to the noted exceptions for reporting withdrawn students. The first relates to inadvertently excluding students on a Leave of Absence from the population of withdrawn students reported to NSLDS and has already been resolved. The second issue is the exclusion of students who have dropped all credits, but have not notified Mason of intent to withdraw. Mason will modify operations and business practices to code students as withdrawn for reporting to NSLDS if they drop all their credits whether or not they have notified Mason of their intent to withdraw. This change is expected to be completed by May 2021.

APA Finding - Implement Third-Party Service Provider Oversight Process

The University developed and began implementing a service provider oversight process in December 2020 to gain annual assurance that all information technology (IT) service providers (providers) have effective operating controls to protect the University's critical and confidential data. However, the University has not yet requested and reviewed independent audit reports, such as System and Organization Controls (SOC) reports, or an acceptable substitute, from each provider across all hosted systems.

Specifically, the University has not obtained a SOC report or an acceptable substitute for four of the 21 providers hosting protected data classified as highly sensitive data (HSD). The University also has not obtained audit assurance from the 16 providers hosting protected data classified as restricted data. Additionally, the University has not completed documentation of control deficiencies, along with mitigating controls, for 17 of the 21 providers hosting protected data classified as HSD or for any of the 16 providers hosting protected data classified as restricted data.

The University's Third-Party Risk Management Process document requires that the University request and evaluate annual security assessment reports from providers, identify compliance gaps, develop mitigation plans, and escalate issues of non-compliance. The University's security standard, the National Institute of Standards and Technology Standard, 800-53 (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).

Due to resource restraints, the University determined to initially target completing the process for providers hosting protected data classified as highly sensitive data. By not fully implementing the process to gain assurance over all 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 should dedicate the necessary resources to complete its efforts to request and evaluate annual security assessment reports from each provider to ensure the provider has effective operating controls to protect the University's sensitive and confidential data. During the evaluation, the University should identify control deficiencies, develop mitigation plans, and escalate issues of non-compliance, as needed. By gaining assurance over each provider, the University will help to ensure the confidentiality, integrity, and availability of sensitive data.

Management's Response

The University began implementing new controls over service providers in 2016 and has been developing and maturing the program since that time. The program is taking time to implement as most of the vendor security audit reports are being evaluated for the first time. Management intends to modify the current program to classify service providers into tiers based on relative risk and criticality, with specified security assessment requirements per tier. The updated program is planned to be in full operation no later than January 31, 2022.

APA Finding - Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act

The University does not implement cybersecurity requirements of the Gramm-Leach-Bliley Act (GLBA) for some systems containing customer information in accordance with the Code of Federal Regulations and University policy. The University completed a System Security Plan (SSP) that identify risks to the security, confidentiality, and integrity of customer information and assess the safeguards in place to control these risks for two systems, including the financial system of record that stores student and financial data. However, the University has not evaluated each of their systems to determine what systems contain customer information. The University also has not completed a sensitive systems list and completed an SSP for each system on the sensitive systems list.

The Code of Federal Regulations, Part 314.4, requires that organizations develop, implement, and maintain the information security program to safeguard customer information and complete a risk assessment that includes consideration of risks in each relevant area of operation. The Information Technology Security Program policy requires that all employees, students, visitors, and contractors must comply with the Information Technology Security Standard. The Information Technology Security Standard requires that the University develop and maintain a SSP for each sensitive system that assesses the system environment and controls.

Without implementing cybersecurity requirements of the GLBA for each system containing customer information, the University may not be able to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The University completed its new Information Technology Security Standard in July 2019 after transitioning from ISO 27002 to the NIST 800-53 Security Standard. The University then began a plan to evaluate each of their systems to determine what systems contain customer information and complete an SSP for each system. However, due to resource constraints and project prioritization, the University has not yet conducted the risk evaluations and implemented the controls necessary to meet the cybersecurity requirements of the GLBA for each system containing customer information.

The University should evaluate their systems to determine what systems contain customer information, then document a sensitive systems list and complete an SSP for each system on the list. Doing this will protect the security, confidentiality, and integrity of customer information and meet the requirements set forth in the GLBA.

Management's Response

The University's Information Technology Security Office maintains an inventory of sensitive servers and devices, categorized by risk and impact based on the type of data they contain or functions they support. The inventory does not yet include a higher-level aggregated view that identifies the "systems" that are comprised of those devices. As APA indicates, the University's recently adopted IT Security Standard requires a System Security Plan to be developed for each "sensitive system." To comply with the requirements of the Security Standard and the GLBA, the Information Technology Security Office will work with departments and data stewards to document systems boundaries and supporting elements, and create System Security Plans for those that meet the criteria of the Standard. This effort will be completed by December 31, 2021.

APA Finding - Improve Security Awareness Training

The University is not meeting certain requirements in the 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 information 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.

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, 2020

BOARD OF VISITORS

Thomas M. Davis, Rector

James W. Hazel, Vice Rector

Horace Blackman, Secretary

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

UNIVERSITY OFFICIALS

Anne Holton, Interim President

Carol Kissal, Senior Vice President for Administration and Finance

Deb Dickenson, Vice President of Finance

Sharon Heinle, Associate Vice President and Controller