NORFOLK STATE 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 Norfolk State University as of and for the year ended June 30, 2019, and issued our report thereon, dated June 12, 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 Norfolk State's website at www.nsu.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 findings entitled "Improve Reporting to National Student Loan Data System," "Properly Process Title IV Refund Calculations," and "Improve Notification Process for Title IV Awards to Students," because the University was in the process of implementing corrective action during our audit period. We will follow up on these findings during the fiscal year 2020 audit. The University has taken adequate corrective action with respect to the remaining audit findings reported in the prior year that are not repeated in this report.

– TABLE OF CONTENTS –

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Continue to Improve Information Security, Risk Management and Contingency Programs

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2016)

In prior year audits, we recommended that Norfolk State University (University) improve oversight over the information security program to ensure it meets or exceeds the requirements of the Commonwealth's Information Security Standard, SEC 501 (Security Standard). The University has made progress to improve its information security program by updating the Business Impact Analysis and developing risk assessments for sensitive systems. Additionally, the University is updating and consolidating its policies and procedures to align with the requirements of the Security Standard. The University should continue efforts to improve the overall security program by updating information technology (IT) continuity of operations (COOP) and IT disaster recovery plans (DRP).

The Security Standard, Section 2.4.2, requires the agency head to ensure an information security program is maintained, that is sufficient to protect the agency's information technology systems, and that is documented and effectively communicated. Section 2.5.1 requires the Information Security Officer to maintain sufficient oversight over the information security program to ensure that it meets or exceeds the requirements of the Security Standard. Additionally, the University is not meeting the requirements in the entire Contingency Planning and Risk Assessment Sections of the Security Standard. *(Section 1.6 Family: Contingency Planning and Section 1.14 Family: Risk Assessment)*.

By not having a comprehensive information security program the University cannot adequately protect its systems against known vulnerabilities that may affect data confidentiality, integrity, or availability. In addition, by having out-of-date and incomplete COOP and DRP plans the University may not be able to bring sensitive and mission critical systems online in a timely manner if a disaster occurs.

The University should continue to implement its corrective action plan and maintain an information security program that meets the requirements in the Security Standard. The University should update its procedures and develop a risk management and contingency management process that consistently addresses and mitigates risks to its sensitive data. Having a complete information security program that includes current policies, and current risk management and contingency management programs will help to ensure that the University can adequately protect sensitive systems and bring systems online in a timely manner to resume normal business operations.

Continue to Upgrade or Decommission End-of-Life Technology

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2015)

The University continues to utilize end-of-life technologies in its IT environment. The University has reduced the number of end-of-life technologies but still maintains technologies that its vendor no longer supports. We have communicated this information to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing specific descriptions of security mechanisms. The Security Standard, Section SI-2-COV, prohibits agencies from using software which the vendor no longer supports. The University should dedicate the necessary resources to evaluate and upgrade or decommission the remaining end-of-life technologies.

Comply with Prompt Payment Provisions

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

During fiscal year 2019, the University did not process a number of payments in compliance with the prompt payment provisions of the Virginia Public Procurement Act (VPPA). In our sample of thirty vouchers, we identified five instances (16.67%) where the University did not process the payment within the required thirty days.

Code of Virginia § 2.2-4350 requires state agencies to pay for delivered goods and services within thirty calendar days after receipt of a proper invoice, or thirty days after receipt of the goods or services, whichever is later. Not following prompt payment requirements established by the Code of Virginia may harm the University's reputation as a buyer, damage relationships with vendors, and could result in late fees.

In the cases noted above, late payment was primarily a result of delays by individual departments in updating purchase orders or approving timesheets detailing vendor labor hours. Without an accurate and properly approved purchase order, or approval of vendor labor charges, accounts payable cannot process payment for the respective vendor charges.

The University should ensure Accounts Payable processes all vendor payments in compliance with the prompt payment provisions of the VPPA. To support this, the University should improve processes to ensure that departments timely approve and submit required documentation to Accounts Payable to ensure all payments can be made within the thirty-day period.

Improve Employee Termination Procedures

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

Upon the separation of an employee from the University, departments are not timely completing the termination checklists, resulting in untimely removal of user access to the University's network and systems. Our audit of the termination process identified the following:

- We sampled 11 employees who separated from the University during fiscal year 2019 and found two employees (18%) who continued to have University network access for more than 24 hours, after separation.

- Nine employees terminated during fiscal year 2019 had access to the Commonwealth's procurement system. Eight of these employees (88%) continued to have access to the procurement system for more than 24 hours after separation.

The Security Standard *(Section PS-4a)* states that an organization must disable information system access within 24 hours of employment termination. Untimely removal of user access increases the risk of unauthorized transactions and access that can compromise the integrity of the University's internal systems, including its financial system.

The University's current account management policy does not align with the Security Standard by not including a requirement to remove access within 24 hours of termination. The University should update the current employee separation and account management polices to ensure compliance with the Security Standard. Additionally, Human Resources and the Office of Information Technology should provide training to all supervisors to confirm everyone is aware of their responsibilities related to the employee separation and system access removal process.

Complete Purchase Card Reconciliations Timely

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Small Purchase Charge Card (SPCC) cardholders at the University's are not timely performing charge card reconciliations. Based on a sample of cardholder reconciliations for fiscal year 2019, three out of fourteen reconciliations (21%) were not prepared and approved timely.

The University's SPCC policy states that cardholders are to submit their completed reconciliation, which includes certifying signatures from the cardholder and their supervisor, to the Accounts Payable Department no later than the 1st of the month following the card statement. Additionally, the

Commonwealth's SPCC policy states that individual SPCC monthly reconciliations are to be prepared before receipt of the following month's card statement.

Untimely completion of the SPCC reconciliations increases the University's risk of not detecting unauthorized or accidental charges in a timely manner. The SPCC Administrator should make efforts to ensure that cardholders are completing reconciliations timely, and that supervisors approve reconciliations timely. The SPCC Administrator should monitor and enforce compliance with the University's SPCC policies and procedures.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 12, 2020

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
Norfolk State 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 the **Norfolk State 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 June 12, 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's 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 opinions 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, "Continue to Improve Information Security, Risk Management, and Contingency Programs," "Continue to Upgrade or Decommission End-of-Life Technology," "Comply with Prompt Payment Requirements," "Improve Employee Termination Procedures," and "Complete Purchase Card Reconciliations Timely," 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 "Continue to Improve Information Security, Risk Management, and Contingency Programs," "Continue to Upgrade or Decommission End-of-Life Technology," "Comply with Prompt Payment Requirements," and "Improve Employee Termination Procedures."

The University's Response to Findings

We discussed this report with management at an exit conference held on July 2, 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 prior audit findings entitled "Improve Reporting to National Student Loan Data System," "Properly Process Title IV Refund Calculations," and "Improve Notification Process for Title IV Awards to Students," because the University did not implement corrective action during our audit period. We will follow up on these findings during the fiscal year 2020 audit. The University has not completed adequate corrective action with respect to the previously reported findings "Improve Information Security, Risk Management, and Contingency Programs" and "Continue to Upgrade or Decommission End-of-Life Technology." Accordingly, we included these findings in the section entitled "Internal Control and Compliance Findings and Recommendations." 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 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

JMR/clj

NORFOLK STATE UNIVERSITY

We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

June 12, 2020

Ms. Martha Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Mavredes:

Norfolk State University has reviewed the Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the fiscal year ending June 30, 2019 and agrees, in principle, with all of the findings.

Attached for your consideration is a brief update as to where the campus is with respect to the findings. The formal Corrective Action Workplan will be submitted within thirty days as required by CAPP Manual Topic No. 10205. Please contact me should you have any questions or require additional information.

On behalf of Norfolk State University, please extend my appreciation to all of your staff for their professional audit work and recommendations.

Sincerely,

Gerald E. Hunter
Vice President for Finance and Administration

Cc: Javaune Adams-Gaston, Ph.D., President
Justin Moses, J.D., Ed.D., VP for Operations & Chief Strategist for Institutional Effectiveness
Karla Amaya Gordon, AVP for Finance and Administration / University Controller
Harry Aristakesian, University Internal Auditor
S. Faye Monroe-Davis, Chief Information Officer
Karen Pruden, Ph.D., AVP for Human Resource
Ruby Spicer, Director of Procurement Services

An Equal Opportunity Employer

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

FY 2019 – Internal Control & Compliance Findings
Management Response

Continue to Improve Information Security, Risk Management and Contingency Programs

The Norfolk State University Office of Information Technology (OIT) made significant improvements in the Information Security Program, including Risk Management and Contingency Planning. Building upon this robust security foundation, the Security Program and Framework provides continuous security assessments for all new and existing business processes and supporting Information Technology (IT) systems; and addresses roles, responsibilities, management commitment, coordination among organizational entities, and compliance with Commonwealth of Virginia Information Technology Resource Management (ITRM) Security Standard SEC501 for identified sensitive IT systems. With the support of VITA ISO Services, the Security Program and Framework completed the University-wide Business Impact Analysis (BIA), identification of essential business processes and IT systems, and classification of data types. Presently, OIT is completing scheduled IT system Risk Assessments and Security Audits for identified sensitive systems. Furthermore, the Security Program and Framework are repeatable processes that assess the risk and security controls throughout the life cycle of critical business processes and related IT systems. Overall outcomes of the Security Program will continuously improve inputs to Norfolk State University IT Continuity of Operations (COOP) and IT Disaster Recovery Plans (DRP) that provide ongoing planning and forecasting activity. In parallel efforts, Norfolk State University is consolidating and updating Security Policies and providing continuous training to staff members who hold key security roles and responsibilities. Additionally, policy updates are scheduled to be completed by December 31, 2020.

Continue to Upgrade or Decommission End-of Life Technology

Norfolk State University continues to upgrade and decommission end-of-life technology projects and employ additional IT professionals to facilitate these projects. These projects are scheduled to be completed by December 31, 2020.

Comply with Prompt Payment Provisions

The Office of the Controller, in conjunction with the Procurement Office, will continue to provide training and education for budget managers and fiscal staff throughout the University, including timely receipt of goods and services within the University's Colleague financial system and providing Accounts Payable the appropriate authorization time to pay accounts. The training and education is provided through the Finance and Administration forums and newsletters. In addition, all training and education materials from the Finance and Administration forums are accessible 24/7 on the University intranet (MYNSU) under Faculty and Staff Resources.

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

Improve Employee Termination Procedures

The University's Office of Information Technology (OIT) department has completed the Logical Access Control policy that aligns with SEC 501 Security Standard to disable access of terminated employees within 24 hours, once notified by Human Resources (HR). The Logical Access Control policy is currently in the University's approval process for campus distribution.

When a supervisor initiates the clearance form notifying HR that the employee electronic clearance process has commenced, HR is responsible for accepting it within 72 hours of receipt. Once accepted by HR, the employee clearance form is automatically deployed to registered departments, including OIT, to take appropriate action.

HR will continue to provide training and education for hiring managers and supervisors on the University's employee electronic clearance form processes. To supplement, upon notification of termination, HR sends a reminder to the supervisors to complete the form. If the supervisor does not complete the form, HR initiates the clearance form for the terminated employee. Additionally, a monthly termination listing from the University's Personnel Management Information System will be provided to the OIT as a secondary method to ensure access is terminated timely. The monthly listing will be monitored through the President's Office Compliance tracking.

Complete Purchase Card Reconciliation Timely

The NSU Procurement Office has completed steps to improve and strengthen the Program Management responsibilities, including the following:

- Strengthen and updated the internal SPCC policy.
- Developed systematic review processes that closely monitor activity.
- Revised reconciliation submission procedures to ensure timely submission.
- Implemented online reconciliation process through Bank of America that provides real time review of cardholder transactions.

NORFOLK STATE UNIVERSITY

As of June 30, 2019

BOARD OF VISITORS

Joan G. Wilmer, Sr., Rector

Dr. Deborah M. DiCroce, Vice Rector

Devon M. Henry, Secretary

Dr. Ann A. Adams	B. Keith Fulton
Dwayne B. Blake	Larry A. Griffith
Kenneth W. Crowder	Michael J. Helpinstill
Jean W. Cunningham	Devon M. Henry
James W. Dyke, Jr.	Joan G. Wilmer

Dr. Tamara A. Jones

UNIVERSITY OFFICIALS

Dr. Melvin T. Stith, Sr., Interim President *(through June 23, 2019)*

Dr. Javaune Adams-Gaston, President *(effective June 24, 2019)*

Dr. Carl W. Haywood, Chief of Staff

Dr. Leroy Hamilton, Jr., Interim Provost and Vice President for Academic Affairs

Gerald E. Hunter, Vice President for Finance and Administration

Dr. Deborah C. Fontaine, Vice President for University Advancement

Dr. Michael M. Shackleford, Vice President for Student Affairs and Enrollment Management

Ericke S. Cage, Executive Advisor to the President and Board of Visitors for Policy, Compliance and University Ombudsman

Marty L. Miller, Athletics Director

Pamela F. Boston, Esq., University Counsel

Harry Aristakesian, Chief Audit Executive