NORFOLK STATE UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2016

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, 2016, and issued our report thereon, dated June 20, 2017. Our report, included in Norfolk State'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 of Norfolk State University for the year ended June 30, 2016, 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.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS

Properly Reflect Enrollment Changes in the National Student Loan Data System

In our last audit, we recommended that Norfolk State University (University) improve reporting of withdrawal statuses submitted to the National Student Loan Data System (NSLDS). The University was not ensuring the withdrawn statuses in the NSLDS populated correctly for the students who have withdrawn from the University. A student's enrollment status determines eligibility for in-school status, as well as loan deferment and grace periods. Enrollment reporting is not only critical for effective administration of the Title IV student loan programs, but is also required so that the U.S. Department of Education (ED) can engage in budgetary and policy analysis.

The University has implemented new controls, including weekly checks of the National Student Clearinghouse system, to ensure enrollment status changes are accurately reflected. This corrective action was considered ongoing in the Commonwealth of Virginia Single Audit Report for the year ended June 30, 2016. We will review the implementation of the University's corrective action during our next audit.

Promptly Remit Unclaimed Federal Student Aid Funds

In our last audit, we recommended that the University improve the process related to the return of unclaimed federal student aid to ED. The University was not returning unclaimed federal student aid checks to ED within 240 days of issuing a check to the student. Not returning the unclaimed checks timely can result in noncompliance with federal student aid program requirements.

The University has implemented new procedures to ensure all outstanding checks are researched timely and federal student aid funds are returned within the 240-day requirement when not cashed by the student. This corrective action was considered ongoing in the Commonwealth of Virginia Single Audit Report for the year ended June 30, 2016. We will review the implementation of the University's corrective action during our next audit.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Information System Security Findings

Norfolk State University is responsible for managing several sensitive information technology (IT) systems, including an enterprise resource planning system. Due to the sensitivity of the data, the University must implement the necessary controls to ensure the confidentiality, integrity, and availability of the data within the various systems. The University has experienced turnover in several key IT positions including the Chief Information Officer and Chief Information Security Officer. The University should obtain the necessary resources, including but not limited to filling vacant positions in the Office of Information Technology, to update and manage the information security program. Additionally, the University should continue to work with the Virginia Information Technologies Agency to ensure audits are performed over all sensitive systems. Our review of information system security resulted in the following four recommendations.

Improve Information Security, Risk Management and Contingency Programs

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

The University is not maintaining sufficient oversight over the information security program to ensure it meets or exceeds the requirements of the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard). The University does not have a sufficient risk management and contingency program to support and protect its sensitive systems. The University's policies and procedures are three years old and align with the requirements in the previous Security Standard version that dates to April 2014. The University does not have risk assessments for any of its sensitive systems and has incomplete and out-of-date continuity of operations (COOP) and disaster recovery plans (DRP). The COOP and DRP documents are over three years old, do not reflect the current information technology (IT) environment, have not had annual tests to ensure validity, and list employees in key recovery roles that are no longer with the University.

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 maintain sufficient oversight over the information security program to ensure that it meets or exceeds the requirements of the Security Standard. In addition, the University is not meeting the

requirements in the entire Contingency Planning and Risk Assessment Sections of the Security Standard *(Section 8.6 Family: Contingency Planning and Section 8.14 Family: Risk Assessment).*

Turnover and a lack of resources led to the current weaknesses in the information security, risk management and contingency programs. By not having a comprehensive information security program and risk assessments on sensitive systems, the University cannot adequately protect their sensitive 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 develop a plan to implement and maintain an information security program that meets the requirements in the current Security Standard and develop a risk management process that accurately and consistently addresses risks to the University's sensitive systems. The University should evaluate and assign the resources necessary to help ensure the University can adequately protect sensitive systems and bring systems online in a timely manner so the University can resume normal business operations.

Conduct Information Technology Security Audits on Sensitive Systems

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

The University is not performing timely IT security audits of its sensitive systems in accordance with the Commonwealth's IT Security Audit Standard, SEC 502-02 (IT Audit Standard). The University has a contract with the Virginia Information Technologies Agency (VITA) to perform audits for the University's sensitive systems. The University's contract for audit services began in fiscal year 2017, and to date the University has not received any services from VITA. VITA plans to perform audits on the University's sensitive systems by August 2018.

The IT Audit Standard, Section 1.4, requires that IT systems containing sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Without conducting IT security audits timely, the University increases the risk that IT staff will not detect and mitigate existing weaknesses in sensitive systems, which increases the risk of malicious parties compromising sensitive and confidential data.

The University should continue to work with VITA to ensure they perform IT security audits on a consistent and timely basis for each sensitive system in accordance with the IT Security Audit Standard.

Continue to Upgrade or Decommission End-of-Life Technology

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes
Prior Title: Improve IT Server Maintenance and Management Controls

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 support mission essential data on IT systems running outdated software that its vendor no longer supports. We have communicated this information in detail to management 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 controls.

The Security Standard, Section SI-2-COV, prohibits agencies from using software that is no longer supported by its vendor. Turnover at key positions and the lack of IT resources delayed the University's plans to decommission or upgrade the end-of-life technology. The University's Chief Information Officer and Chief Information Security Officer are aware of these weaknesses and have plans to upgrade all the end-of-life technologies by August 2017. The University should dedicate the necessary resources to evaluate and implement the controls and recommendations discussed in the communication marked FOIAE in accordance with the Security Standard.

Improve IT Asset Surplus and Sanitization Controls

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

The University lacks documented IT asset sanitization procedures and a quality assurance process. The University does not use some required controls to protect IT assets prior to transfer or removal from service. We identified and communicated this information to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing specific descriptions of security mechanisms.

The Information Technology Resource Management Standard for Removal of Commonwealth Data from Electronic Media, SEC 514-04 (Data Removal Standard), requires the University to have procedures that appropriately document the entire data removal process prior to the physical transfer or destruction of an IT asset. The Data Removal Standard also requires the University to develop and implement a documented quality assurance process to test for effective data removal from electronic media.

The University should dedicate the necessary resources to implement the controls and recommendations discussed in the communication marked FOIAE in accordance with the Data Removal Standard.

Other Finding

Comply with 1500 Hour Rule for Wage Employees

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

The University is not complying with Chapter 732, §4-7.01, of the 2016 Virginia Acts of Assembly. The University is responsible for implementing policies and procedures to ensure employees who are not eligible for benefits do not work more than 29 hours per week on average over a 12-month period. Two non-benefited employees exceeded the 29-hour average for the period May 1, 2015, to April 30, 2016.

Chapter 732, §4-7.01, of the 2016 Virginia Acts of Assembly limits non-benefited employees to working no more than an average of 29 hours per week in the one-year measurement period of May 1 to April 30. The Commonwealth developed this policy to ensure compliance with the requirements of the Affordable Care Act, which could bring penalties for noncompliance.

Due to the variety of employee types at the University, and employees working multiple positions, tracking employees' hours to ensure compliance with the 29-hour average limit will require strong internal controls. To avoid penalties and ensure compliance with state and federal requirements, the University should follow policies and procedures to assist in monitoring non-benefited employees to ensure hours do not exceed an average of 29 hours per week over the course of the year. Additionally, the University should monitor a standardized report of all non-benefited employees' hours and alert supervisors as they approach the limit. This will greatly reduce the risk of non-compliance.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 20, 2017

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
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, the aggregate discretely presented component units of **Norfolk State University** (the University) as of and for the year ended June 30, 2016, 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 20, 2017. 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 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 "Properly Reflect Enrollment Changes in the National Student Loan Data System" and "Promptly Remit Unclaimed Federal Student Aid Funds," which are described in the section entitled "Status of Prior Year Findings;" along with the findings entitled "Improve Information Security, Risk Management and Contingency Programs," "Conduct Information Technology Security Audits on Sensitive Systems," "Continue to Upgrade or Decommission End-of-Life Technology," "Improve IT Asset Surplus and Sanitization Controls" and "Comply with 1500 Hour Rule for Wage Employees," 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 "Improve Information Security, Risk Management and Contingency Programs," "Conduct Information Technology Security Audits on Sensitive Systems," "Continue to Upgrade or Decommission End-of-Life Technology," "Improve IT Asset Surplus and Sanitization Controls" and "Comply with 1500 Hour Rule for Wage Employees."

The University's Response to Findings

We discussed this report with management at an exit conference held on June 21, 2017. 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

The University is taking adequate corrective action with respect to audit findings reported in the prior year that are reported in the section entitled “Status of Prior Year Findings.” The University has not taken adequate corrective action with respect to the previously reported finding “Improve IT Asset Surplus and Sanitization Controls.” Additionally, the University has partially corrected the previously reported finding “Improve IT Server Maintenance and Management Controls.” 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.

AUDITOR OF PUBLIC ACCOUNTS

MR/alh

NSU
NORFOLK STATE UNIVERSITY

Vice President for Finance and Administration
700 Park Avenue, Suite 310, Norfolk, Virginia 23504
Tel: (757) 823-8011 Fax: (757) 823-8048
Web: www.nsu.edu

June 20, 2017

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

Dear Ms. Mavredes:

Norfolk State University has reviewed the Financial Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the fiscal year ending June 30, 2016 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: Mr. Eddie N. Moore Jr., President / CEO
Dr. Stacey Franklin Jones, Interim Provost and Vice President for Academic Affairs
Mrs. Karla Amaya Gordon, AVP of Finance and Administration / University Controller
Mr. Harry Aristakesian, University Internal Auditor

FY 2016 – Financial Internal Control & Compliance Findings

Improve Information Security, Risk Management and Contingency Programs

Norfolk State University will ensure efficient oversight of its Information Security Program to ensure it meets or exceeds the requirements of the Commonwealth of Virginia's Security Standard SEC501-09.1 dated December 8, 2016. The University will ensure the Information Security Program is maintained and protects the University's information systems and is effectively documented and communicated in accordance with section 2.4.2 of the Security Standard. A formal process has been put in place that adheres to the Commonwealth's and the University's policy. Additionally, the University will ensure an efficient risk management process is implemented that consistently addresses risks to sensitive systems and complies with sections 8.6 Family: Contingency Planning and 8.14 Family: Risk Assessment of the Security Standard. The University currently has a MOU with VITA that will assist in implementing these programs and perform audits of its sensitive systems. Work has already begun on updating the Continuity of Operations (COOP) plan and Disaster Recovery Plan (DRP), which reflects the current environment. In accordance with the Security Standard, annual testing to ensure validity of the plans will be completed.

Conduct Information Technology Security Audits on Sensitive Systems

Norfolk State University will implement a process to perform timely IT Security Audits of its sensitive systems in accordance with the Commonwealth's IT Security Audit Standard SEC502-02. The University currently has a MOU with VITA that will assist in implementing the Security Audit program and perform audits of its sensitive systems. Work has already begun with VITA on implementing this plan. We are currently identifying sensitive systems, documenting the plan and building a schedule to audit our systems. This plan will ensure that audits will occur on a timely basis and IT staff will detect and mitigate potential weaknesses in sensitive systems.

Continue to Upgrade or Decommission End-of Life technology

Norfolk State University has implemented a process to upgrade or decommission end-of-life technology. VITA has released our new infrastructure hardware for procurement. New equipment has been purchased that will satisfy this requirement. We are currently in the process of obtaining updated software that will operate on the new hardware. Schedules have been put in place that will ensure timely replacement of end-of-life hardware.

Improve IT Asset Surplus and Sanitization Controls

Norfolk State University has drafted procedures that align with the Information Technology Resource Management Standard for Removal of Commonwealth Data from Electronic Media (SEC514). As part of our Information Security MOU with VITA we are reviewing content to formalize the document while ensuring compliance with the security standard.

Comply with 1500 Hour Rule for Wage Employees

To ensure the University complies with the 1500-hour regulation, hourly employees work an average of 29 hours per week as stated in offer letters. A monitoring report is currently run and reviewed monthly by the Office of Human Resources. Once the employee has reached 500 hours, the Office of Human

Resources sends an email reminder/warning to the employee's supervisor and the employee; as well as send emails bi-weekly as the hours available decrease. The University has put this corrective action in place to comply with Chapter 732 §4-7.01 g of the 2016 Virginia Acts of Assembly. Additionally, the 1500-hour monitoring report will be included on the University's Compliance Report that is tracked monthly by the President's Office.

NORFOLK STATE UNIVERSITY

Norfolk, Virginia
As of June 30, 2016

BOARD OF VISITORS

Dr. Byron L. Cherry, Sr., Rector

Dr. Melvin T. Stith, Vice Rector

Lula B. Holland, Secretary

Dr. Ann A. Adams
Elwood B. Boone, III
Thomas N. Chewning
Kenneth W. Crowder
Bryan D. Cuffee
Dr. Deborah M. DiCroce
Larry A. Griffith
Michael J. Helpinstill
Beth Murphy
Michael D. Rochelle

OFFICIALS

Eddie N. Moore, Jr., President and CEO

Dr. Sandra J. Deloatch, Provost and Vice President for Academic Affairs

Gerald E. Hunter, Vice President for Finance and Administration

Edward M. Willis, Vice President for Student Affairs

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

Clementine S. Cone, Executive Assistant to the President for University Compliance

Dr. Paula Gentius, Executive Policy Advisor to the President and Board of Visitors

Dr. Michael M. Shackleford, Associate Vice President for Enrollment Management

Mona Adkins-Easley, Associate Vice President for Human Resources

Marty L. Miller, Athletics Director