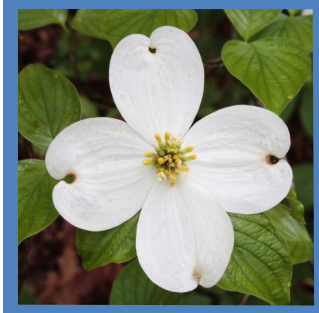


NORFOLK STATE UNIVERSITY

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

Commonwealth of Virginia
APA
Auditor of Public Accounts

AUDIT SUMMARY

We have audited the basic financial statements of Norfolk State University as of and for the year ended June 30, 2020, and issued our report thereon, dated May 12, 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 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.

Our audit also included testing over the major federal program of the 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.

We did not perform audit work related to the prior audit finding and recommendation entitled "Improve Reporting to National Student Loan Data System," because the University was in the process of implementing corrective action during our audit period. We will follow up on this finding during the fiscal year 2021 audit.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR 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, with limited progress in this area)

Norfolk State University (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 (Security Standard) and does not have a sufficient risk management and contingency program to support and protect its sensitive systems. Specifically, the University does not:

- have or ensure risk assessments exist for all sensitive information technology (IT) systems; and

- have continuity of operations (COOP) and disaster recovery plans (DRP) for the IT systems that support mission essential functions and processes.

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. Furthermore, Section 2.5.1 requires the Information Security Officer (ISO) to maintain sufficient oversight over the information security program to ensure that it meets or exceeds the requirements of the Security Standard. Lastly, the University is not meeting some requirements in the Contingency Planning and Risk Assessment sections of the Security Standard (Section 6 Risk Assessment, Section 8.14 Family: Risk Assessment, Section 8.6 Family: Contingency Planning).

Without maintaining effective IT risk management and contingency planning documentation, the University puts at risk the ability to recover the essential and primary business functions required to operate effectively in the event of an emergency or disaster, which could lead to monetary or reputational damages for the University. By not completing a risk assessment for each sensitive system and not performing timely reviews, the University also risks not identifying and addressing new or changing threats. In addition, by not having an official COOP for all its mission essential business functions or a DRP for IT systems that support those functions, the University may not be able to bring sensitive and mission critical systems online in a timely manner if a disaster occurs.

Turnover and a lack of resources led to the University having out-of-date policies and lacking current risk management and contingency management programs. This recommendation has been an ongoing concern and originally identified in our audit for fiscal year 2016. In 2016, the University obtained ISO services from the Virginia Information Technologies Agency (VITA) to assist in the process of developing IT risk management and contingency planning documentation; however, these services have not progressed as planned. During fiscal year 2019, the University completed the Business Impact

Analysis. During fiscal year 2020, the University completed the risk assessment process for nine of the 19 sensitive systems, of which only four of nine have been processed by VITA. By not having a comprehensive risk management and contingency program for sensitive systems, the University cannot adequately protect against known vulnerabilities that may affect data confidentiality, integrity, or availability.

The University should continue to implement their corrective action plan and maintain an information security program. The University should update their 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.

The University should dedicate the necessary resources to improve its risk management and contingency management processes, such that it meets the requirements in the Security Standard. Additionally, the University should develop a plan with VITA to expedite the completion of all the outstanding risk assessments. Further, the University should dedicate the necessary resources to prioritize the development of their COOP and IT DRP. Completing corrective action will help to ensure the University protects the confidentiality, integrity, and availability of its sensitive and mission critical systems.

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, with limited progress in this area)

The University continues to use end-of-life and unsupported software in a portion of its IT environment. The University's Office of Information Technology (OIT) has updated, replaced, or retired some unsupported software on several IT systems since our last review, and OIT has plans to continue to upgrade and decommission unsupported software during 2021.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard prohibits agencies from using software that is end-of-life and no longer vendor supported to reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should dedicate the necessary resources to evaluate and implement the controls and recommendations discussed in the communication marked FOIA Exempt in accordance with the Security Standard. Implementing corrective action will increase the University's security posture and help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Comply with Prompt Payment Provisions

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

During fiscal year 2020, the University failed to process payments in compliance with the prompt payment requirements of the Virginia Public Procurement Act (VPPA). In our sample of 26 vouchers for which prompt payment requirements were applicable, we identified eight instances (30.77%) in which the University did not process payment within the required 30 days.

Section 2.2-4350 of the Code of Virginia requires state agencies to pay for delivered goods and services within 30 calendar days after receipt of a proper invoice, or 30 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.

Late payment was primarily a result of delays by individual departments in updating purchase orders or informing Accounts Payable of payment authorization on invoices. Without an accurate and properly approved purchase order or an authorization of payment from the purchasing department, 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 requirements of the VPPA. To achieve compliance, the University should improve processes to ensure that departments approve and submit required documentation in a timely manner to Accounts Payable to ensure all payments can be made within the 30-day period. Additionally, the University should ensure accurate dates are entered into the Commonwealth's accounting and financial reporting system, so that the University can properly monitor compliance with the prompt payment requirements.

Improve Controls over Purchasing System Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2019)
Prior Title: Improve Employee Termination Procedures

The University did not deactivate terminated employees' access to the Commonwealth's purchasing system in a timely manner. The University's purchasing system Security Officer (Security Officer) did not notify the Commonwealth's Division of Purchases and Supply timely for ten out of 18 terminated employees with purchasing system access (55.6%).

Untimely removal of user access increases the risk of unauthorized transactions that can compromise the integrity of the University's purchasing system. The Commonwealth's Division of

Purchases and Supply's Security Standard, Section 2.10, requires the Security Officer to immediately report the termination of employees with purchasing system access. Additionally, the University's Logical Access Control Policy requires account deactivation within 24-hours of notification of user termination.

Account deactivation delays are primarily a result of untimely notification of employee termination between individual departments, Procurement Services, and the Security Officer. The University should ensure that purchasing system user accounts belonging to terminated employees are deactivated in accordance with its internal policy and the Commonwealth's Division of Purchases and Supply's Security Standard.

Complete Purchase Card Reconciliations Timely

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

In our last audit, we recommended that the University make efforts to ensure that cardholders complete charge card reconciliations timely and that supervisors approve reconciliations timely. The Commonwealth's Small Purchase Charge Card (SPCC) policy states that individual SPCC monthly reconciliations are to be completed before receipt of the following month's card statement.

The University's SPCC Administrator should monitor and enforce compliance with the University's SPCC policies and procedures. Procurement Services transitioned to an online reconciliation process in October 2020 and revised the University's SPCC policy which was approved in February 2021. We will review the implementation of management's corrective action during our next audit.

Properly Process Title IV Refund Calculations

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

The University's Financial Aid personnel did not accurately perform return of Title IV calculations for spring 2020. Due to the University extending spring break, Financial Aid used an incorrect number of days for the return of Title IV calculations. Although the University used an incorrect number of days for all calculations, the errors did not result in any required repayment to the Department of Education (ED) due to ED granting a COVID-19 waiver to all institutions for the spring term. Additionally, we identified one fall 2019 student for whom Financial Aid performed the calculation accurately but did not identify the withdrawal until April 2020.

Code of Federal Regulations, 34 CFR § 668.22 states, when a recipient of Title IV grant or loan assistance withdraws from an institution during a period of enrollment in which the recipient began attendance, the institution must determine the amount of Title IV grant or loan assistance that the

student earned as of the student's withdrawal date and return the money within a reasonable timeframe. The institution must return the amount of unearned funds after the date that the institution determines the student has withdrawn. Failure to comply with the return provisions of the Code of Federal Regulations could result in the initiation of an adverse action by ED. Financial Aid personnel utilize the University's automated system for calculating the percentages of aid earned and unearned by a student. Financial Aid personnel incorrectly entered the start date in the system and the University modified the length of its spring break resulting in an error for all students requiring a return of Title IV calculation in the spring 2020 term. For the remaining error noted, Financial Aid indicated the student was retroactively withdrawn by the Registrar's office, resulting in the delay in identifying the withdrawal and processing the return.

Financial Aid personnel should review their process for determining the number of days for return of Title IV calculations to ensure accuracy of return amounts. Management should place particular emphasis on this review when events occur that impact the standard published scheduled breaks. Management should implement corrective action to prevent future noncompliance including having management review the calendar dates prior to processing withdraws when using the automated system.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

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 of its sensitive systems in accordance with the Code of Federal Regulations and University Information System Security policy. The University defines sensitive systems as those systems with sensitive data, that when compromised with respect to confidentiality, integrity, or availability, could negatively impact the University's operations or individuals' privacy.

While the University incorporates the GLBA cybersecurity requirements in its risk assessment process and system security plans (SSP), the University has completed the documentation for only nine of 19 sensitive systems. As required by 16 C.F.R. § 314.4, organizations must 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.

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 has started their plan to conduct risk assessments, and to complete an SSP, for each of their identified sensitive systems. However, due to resource constraints, the University has not yet completed the risk assessment process or the development of SSP's for all its sensitive systems.

The University should complete the risk assessments and SSP's for all its sensitive systems. The University expects to have the risk assessment process and SSP's complete for all sensitive systems by December 31, 2021. Completing this corrective action will protect the confidentiality, integrity and availability of customer information and meet the requirements set forth in the GLBA.

Improve Virtual Private Network Security

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

The University does not secure some Virtual Private Network (VPN) settings in accordance with both University remote access policy and the minimum requirements in the Security Standard. We communicated the control weaknesses to management in a separate document marked FOIA Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

By not establishing controls and procedures to meet the requirements of the University's administrative policy #32-8-11 (2014) and the Security Standard with respect to remote access controls, the University increases the risk that a malicious party could compromise a user's account and use it to infiltrate the network which could lead to a breach of data, resulting in legal, financial, and reputational damages.

Turnover and a lack of resources led to the University not having the ability to develop and implement additional security applications to adequately enforce the requirements of the Security Standard and the University's administrative policy #32-8-11 (2014). The University should dedicate the necessary resources to adequately address the issues and requirements discussed in the communication marked FOIA Exempt in accordance with the Security Standard. By properly addressing these issues, the University will reduce the risk of malicious users compromising a user's credentials to access sensitive and mission critical systems in the internal network and ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 12, 2021

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 **Norfolk State 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 May 12, 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 opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

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

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control entitled "Continue to Improve Information Security, Risk Management, and Contingency Programs," "Continue to Upgrade or Decommission End-of-Life Technology," "Comply with Prompt Payment Provisions," "Improve Controls over Purchasing System Access," "Complete Purchase Card Reconciliations Timely," "Properly Process Title IV Refund Calculations," "Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act," and "Improve Virtual Private Network Security," which are described in the sections titled "Status of Prior Year Findings and Recommendations" 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 Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations entitled "Continue to Improve Information Security, Risk Management, and Contingency Programs," "Continue to Upgrade or Decommission End-of-Life Technology," "Comply with Prompt Payment Provisions," "Improve Controls over Purchasing System Access," "Properly Process Title IV Refund Calculations," "Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act," and "Improve Virtual Private Network Security."

The University's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on May 14, 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 "Continue to Improve Information Security, Risk Management, and Contingency Programs," "Continue to Upgrade or Decommission End-of-Life Technology," "Comply with Prompt Payment Provisions," "Improve Controls over Purchasing System Access," "Complete Purchase Card Reconciliations Timely," and "Properly Process Title IV Refund Calculations." Accordingly, we included these findings and recommendations in the section entitled "Status of Prior Year Findings and Recommendations."

We did not perform audit work related to the finding and recommendation included in our report dated October 15, 2018, entitled "Improve Reporting to National Student Loan Data System" because the University did not implement corrective action during our audit period. We will follow up on this finding and recommendation during the fiscal year 2021 audit. The University took adequate corrective action for the finding and recommendation entitled "Improve Notification Process for Title IV Awards to Students."

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

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

May 12, 2021

Ms. Stacie Henshaw
The Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Henshaw:

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, 2020, 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, PhD
Vice President for Finance and Administration

Cc: Javaune Adams-Gaston, PhD, President
Justin Moses, J.D., EdD, VP for Operations & Chief Strategist for Institutional Effectiveness
Karla Amaya Gordon, AVP for Finance and Administration / University Controller
Derika Burgess, University Internal Auditor
S. Faye Monroe-Davis, Chief Information Officer
Ruby Spicer, Director of Procurement Services
Juan Alexander, PhD, AVP for Enrollment Management
Melissa Barnes, Director of Financial Aid

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 2020 – Internal Control & Compliance Findings
Management Response

Continue to Improve Information Security, Risk Management and Contingency Programs

As part of NSU's IT Security Program, a repeatable process has been created to identify, document, and assess new and existing applications. As noted by the Auditor, NSU has initiated a plan to carry out this process, which includes Risk Assessments (RAs) and System Security Plans (SSPs) for each identified sensitive system. The COVID-19 pandemic and a change in the on-campus attendance patterns of faculty and staff contributed to a slow-down in progress towards completion of risk assessments and system security plans, but NSU continues to make progress. Management acknowledges that there are internal control deficiencies and is working to address and accomplish the issues noted. Key deliverables, such as resource allocation, specific milestones, and timelines for deliverables are being put into place. NSU expects to have outstanding risk assessments and SSPs for sensitive systems complete by December 31, 2021. NSU is also actively working on updates to the Continuity of Operations and Disaster Recovery Plans.

Continue to Upgrade or Decommission End-of Life Technology

Norfolk State University has made significant progress in upgrading and decommissioning end-of-life technology campus-wide. The initial priority included NSU's sensitive systems, selected to mitigate risk and threats to these systems. These core systems have been upgraded and/or replaced. NSU will continue to upgrade and decommission end-of-life technology for the University's non-critical systems. The process is scheduled to be completed by July 2022.

Comply with Prompt Payment Provisions

The Office of the Controller, in conjunction with the Procurement Office, will continue to provide education for budget managers and fiscal staff throughout the University on the importance of timely receipt of goods and services within the University's Colleague financial system and providing Accounts Payable the appropriate authorization time to pay accounts.

Improve Controls over Purchasing System Access

Procurement Services has implemented a new "eVA User Access" policy which aims to augment the Office of Information (OIT) Logical Access Control policy and the Purchases and Supply's Security Standard, Section 2.10 in an effort to circumvent the increase risk of unauthorized access for terminated eVA users. It is the goal of Procurement Services to immediately address employee terminations upon notification to ensure timely deactivation. Refer to the University's Logical Access Control Policy that has been updated and approved.

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

Complete Purchase Card Reconciliation Timely

The NSU Procurement Office has completed steps to improve and strengthen the Program Management. The SPCC Administrator will continue to monitor and enforce SPCC policies and procedures compliance of the Small Purchase Charge Card (SPCC). Procurement Services transitioned to an online reconciliation process in October 2020 and revised the University's SPCC policy which was approved in February 2021. Transition of Procurement Services to the online banking reconciliation process in conjunction with employing a newly systematic charge card activity review schedule allows for effective oversight of timely completion of charge card reconciliations and transactions.

Properly Process Title IV Refund Calculations

The Financial Aid Office has developed a Certification Form of Countable Days in the Semester to determine the number of days for the return to Title IV calculations. The form will ascertain the following: semester, first day of classes, breaks (start and end dates), last day of classes, number of break days, number of countable days in the semester and the midpoint date for unofficial withdrawals. The form must be accompanied with a copy of the academic year calendar and the Colleague Financial Aid award period set-up screens (AWPD). The Certification Form must be completed for each semester and must be certified by the Return of Title IV Coordinator, Associate Director of Financial Aid, University Registrar, and the Director of Financial Aid. All required signatures must be obtained certifying the accuracy of the dates prior to processing Return of Funds. Additionally, the Director of Financial Aid, Dean of Students, and University Registrar revisited the University's existing Retroactive Withdrawal Policy and have updated to ensure compliance with Code of Federal Regulation, 34 C.F.R § 668.22.

Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act

As NSU continues to improve the Information Security, Risk Management and Contingency Programs detailed in the report, the University will incorporate activities to ensure compliance with the Gramm-Leach-Bliley Act.

Improve Virtual Private Network Security

NSU is on track to implement the required controls by December 31, 2021.

NORFOLK STATE UNIVERSITY

As of June 30, 2020

BOARD OF VISITORS

Joan G. Wilmer, Rector

Deborah M. DiCroce, Vice Rector

Devon M. Henry, Secretary

Dwayne B. Blake	BK Fulton
Mary L. Blunt	Larry A. Griffith
Kim W. Brown	Michael J. Helpinstill
Jean W. Cunningham	Tamara A. Jones
James W. Dyke, Jr.	Harold L. Watkins, II

UNIVERSITY OFFICIALS

Javaune Adams-Gaston, President

Gerald E. Hunter, Vice President for Finance and Administration