New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Compliance With Payment Card Industry Standards

State University of New York

Report 2015-S-65 June 2016

Executive Summary

Purpose

To determine whether selected State University of New York (SUNY) schools are in compliance with Payment Card Industry (PCI) standards and whether SUNY System Administration has provided sufficient guidance to the campuses regarding PCI compliance. The audit covers the period August 25, 2015 to March 22, 2016.

Background

The State University of New York (SUNY) is the largest comprehensive university system in the United States, consisting of 64 institutions and about 460,000 enrolled students. SUNY System Administration (System Administration) acts as the governance arm of the SUNY system, and provides the various SUNY schools with centralized services and support. System Administration also defines various policies and procedures that apply to all State-operated SUNY schools. This includes procedures addressing the actions required of all institutions to protect the confidentiality of sensitive data, including complying with industry standards. System Administration also evaluates schools' system security through the use of internal security-based questionnaires.

All industries that accept credit cards as a method of payment must comply with the Data Security Standards (DSS) established by the PCI Security Standards Council. The PCI DSS is a set of technical and operational requirements designed to protect cardholder data. SUNY schools accept credit cards as a method of payment (e.g., for tuition, housing, and meals), and as such must comply with the PCI DSS to protect against electronic security breaches and theft of payment card data. Entities that do not comply with PCI DSS may be subject to fines and penalties, as well as lose the ability to accept credit card payments.

Key Findings

- SUNY schools were generally knowledgeable about PCI compliance and the need to protect credit card data from unauthorized access; however, we identified areas where system and data controls need to be improved to meet certain compliance standards. Among a range of issues, we identified weaknesses in: the completeness of systems' component inventories; network segmentation; the resolution of compliance deficiencies; and the oversight of affiliated campus organizations.
- Guidance provided by System Administration could be further developed to help assist SUNY schools with addressing and maintaining compliance with PCI DSS requirements.

Key Recommendations

To SUNY Schools visited:

- Implement the recommendations contained in the detailed preliminary reports.

To System Administration:

- Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all SUNY colleges.

- Revise contract templates for affiliates to address PCI DSS regulations and require affiliates' compliance.

Other Related Audits/Reports of Interest

Office of Information Technology Services: Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems (2013-S-58)

State Education Department: Security Over Online Registration Renewal and Teacher Certification (2008-S-154)

State of New York
Office of the State Comptroller

Division of State Government Accountability

June 8, 2016

Nancy L. Zimpher, Ph.D.
Chancellor
State University of New York
353 Broadway
Albany, NY 12246

Dear Dr. Zimpher:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by so doing, providing accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit of the State University of New York entitled *Compliance With Payment Card Industry Standards*. The audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

Background	5
Audit Findings and Recommendations	7
Schools' Payment Card Industry Compliance	7
Guidance and Monitoring From System Administration	11
Recommendations	12
Audit Scope and Methodology	13
Authority	13
Reporting Requirements	13
Contributors to This Report	15
Agency Comments	16

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The State University of New York (SUNY) is the largest comprehensive university system in the United States. Its mission is to provide the people of New York educational services of the highest quality, with the broadest possible access, fully representative of all segments of the population in a complete range of academic, professional, and vocational postsecondary programs. The SUNY system consists of 64 institutions, including research universities, academic medical centers, liberal arts colleges, community colleges, colleges of technology, and an online learning network. In 2014, SUNY schools enrolled a total of about 460,000 undergraduate and graduate students in 7,262 various academic programs.

SUNY's System Administration, located in Albany, is the governance arm of the university system, providing centralized services and support to all SUNY entities. System Administration also issues various University-wide policies providing details on areas such as governance, academic affairs, legal and compliance issues, and facility management.

All industries that accept credit cards as a method of payment must comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council. The PCI DSS is a set of technical and operational requirements that are designed to protect cardholder data and apply to all system components (e.g., network devices, servers, computing devices, applications) that are included in, or connected to, an entity's cardholder data environment. SUNY schools accept credit cards as a method of payment (e.g., for tuition, housing, and meals), and as such must comply with the PCI DSS to protect against electronic security breaches and theft of payment card data. In addition, auxiliary services corporations (affiliates) that operate on SUNY campuses and use school resources to process credit card transactions (e.g., campus bookstores, eateries, alumni associations) must comply with PCI DSS.

The PCI DSS were created by the five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Entities that fail to comply with the PCI DSS could be subject to fines and penalties, and could lose the ability to accept credit card payments. To assist entities in establishing compliance, the PCI DSS provides detailed assessment procedures encompassing the following six areas of system and data controls:

- Build and Maintain a Secure Network (e.g., install and maintain a firewall configuration, remove vendor-supplied defaults for system passwords and other security parameters);
- Protect Cardholder Data;
- Maintain a Vulnerability Management Program (e.g., use anti-virus software);
- Implement Strong Access Control Measures (e.g., restrict physical access to cardholder data);
- Regularly Monitor and Test Networks (e.g., track and monitor all access to cardholder data, regularly test security systems and processes); and
- Maintain an Information Security Policy.

SUNY school departments and affiliates that accept credit card payments must complete a self-

assessment questionnaire (SAQ) as verification of PCI DSS compliance.

System Administration has issued security guidelines in its Information Security Guidelines, Part 1: Campus Programs & Preserving Confidentiality (Guidelines), and evaluates schools' system security through its own security-based questionnaires. System Administration has also implemented a security operations center, which provides vulnerability scanning and penetration testing support to participating schools. Furthermore, in June 2015, System Administration established an Enterprise Risk Management Policy and Program, which has identified PCI compliance as a preliminary high-risk area requiring further analysis by the Program.

Audit Findings and Recommendations

We reviewed selected operational and technical data security controls over the protection of cardholder data at six SUNY schools: one university center, one medical center, and four colleges. While we found officials at each campus to be generally knowledgeable about PCI compliance and the need to protect credit card data from unauthorized access, we also identified areas where certain system and data controls need to be improved to meet compliance standards.

System Administration has issued guidance and provided some support to campuses regarding efforts to ensure the security over confidential data, which includes credit card information. However, we found areas where this guidance could be further developed to better assist schools when addressing PCI DSS requirements. This includes developing guidance on how to properly implement the operational and technical PCI controls associated with the compliance requirements. Furthermore, officials do not monitor school compliance and are unaware of the compliance status of the individual SUNY schools. System Administration, therefore, cannot ensure that all schools that are accepting credit card payments are PCI DSS compliant.

Schools' Payment Card Industry Compliance

We reviewed selected operational and technical data security controls for the protection of cardholder data for six schools. During this review, we identified multiple areas where significant improvements need to be made to more fully address and meet PCI compliance requirements.

Completeness of PCI Inventories

We found that only one school, Campus F, maintained a complete and accurate inventory of its PCI components. As stated in the PCI DSS, "Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without a complete inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards." System components operating without the proper PCI specific security controls significantly increases the risk of unauthorized access to cardholder data.

At the five schools without complete inventories, we identified systems that were used to process credit card data, but were not known to school officials and were not included in any previous inventory listing. These systems were often general purpose workstations used for both credit card processing and general operational activities, including, but not limited to, reviewing email, preparing documents, and browsing the Internet.

For example, we found three systems at one school (Campus A) used for credit card processing that were unknown to the school, including two staff workstations and a public computer terminal. We also found that a server at another school (Campus B) which hosts a web application that collects credit card data for payment processing had not been approved to accept credit card payments by the school's Information Security Office, as required by its Credit/Debit Card Merchant Requirements Policy.

In response to our preliminary findings, officials at both schools noted they would either implement card readers to replace the need for credit card processing on computer terminals or further improve inventory methodologies to ensure the inventory accurately reflects all PCI components for the school.

Lack of Network Segmentation

Network segmentation refers to isolating systems that process credit card data from the remainder of the organization's network. Although network segmentation is not a requirement of PCI DSS, it is strongly recommended as a means to reduce: the scope and cost of a PCI DSS assessment; the cost and difficulty of implementing and maintaining controls; and the risk to an organization. By separating the systems used for credit card processing from the larger, general purpose network, a school can create a more manageable cardholder data environment to implement all necessary PCI DSS security controls.

We found that five of the six SUNY schools we site visited have not followed PCI DSS-recommended best practices to isolate system PCI components from other portions of their networks. During our on-site visits, we identified systems at the five campuses that store, process, or transmit cardholder data on the same network segments with staff workstations and servers. By not isolating systems, the cost to schools for deploying and maintaining PCI DSS controls is increased, given the larger network scope.

In response to our preliminary findings, four of the five schools noted they would consider interim solutions for isolating systems to comply with PCI DSS. For example, officials from one school (Campus C) stated they are in the process of designing and implementing a segmented network to isolate PCI data from traditional network traffic. The fifth school (Campus D) disagreed with our assessment of its network segmentation, citing that it is not a PCI requirement, but rather only a recommended best practice.

Resolving Compliance Deficiencies Timely

Schools often engage with industry experts for support with the PCI compliance process. Qualified Security Assessors (QSAs), for example, are independent security organizations qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. Four schools we visited used a QSA. For two of them – Campus A and Campus D – we found that instances of non-compliance identified in past QSA risk assessments had not been addressed or corrected in a timely manner.

Compliance issues identified at Campus D were still not remediated approximately 16 months after the QSA's initial assessment, including failure to complete an Incident Response Plan and to institute proper segmentation of affiliate computer systems used for credit card processing. In addition, issues existed at Campus A that were identified in a June 2014 QSA assessment, which remained unresolved at the time of our site visit. These included not having the necessary policies and procedures in place and not configuring system components to meet PCI requirements.

In response to our preliminary findings, Campus A officials stated they will continue to work with their QSA to develop strategies for addressing open and unresolved issues, with a planned completion date of April 15, 2016. Campus D officials, however, disagreed with our findings, stating that some of the unresolved QSA issues were the responsibility of its affiliates. We note that this response contradicts the actual QSA report, which states that since Campus D IT staff support those deficient systems, it is the school's (and not solely the affiliates') responsibility to resolve issues identified.

To reduce the risk of breach or compromise, issues of PCI DSS compliance should be addressed and corrected in a timely manner. According to the PCI DSS, when an entity is unable to meet a PCI requirement, a compensating control should be put in place so the risk associated with the original PCI requirement is appropriately offset. By allowing deficient issues to remain without incorporating compensating controls, the risk of system breach – and compromise of cardholder data – still exists. In response to our preliminary findings, school officials often stated that issues identified by the audit team would be remediated as the result of planned work or future projects without instituting any interim compensating controls.

Limited Oversight of Affiliated Organizations

SUNY affiliates, which provide services such as dining and bookstores and maintain relationships with college alumni, often utilize school resources to process credit card transactions. These transactions are completed either by using the school's network to pass credit card data to a service provider via the Internet or by deploying credit card processing systems within the existing IT infrastructure. We determined that schools do not always ensure affiliates are compliant with PCI requirements. At five of the six schools visited, we found significant deficiencies among affiliates' systems, most of which interacted with school IT resources – the school's network, workstations, and servers – for credit card processing activities.

We identified controls in affiliates' systems that did not appropriately or fully address PCI requirements. We reported these matters to the schools in detailed preliminary findings and, consequently, do not address them in detail in this report due to their confidential nature. While not directly responsible for these deficiencies, by not identifying and addressing them, the schools expose themselves to unnecessary risks should a breach occur. These risks include not only loss or interruption of operations and services, but also potential fines or penalties levied by the affiliate's bank if it is determined the school shares any responsibility for the security incident. Furthermore, a compromise or breach at one of the affiliates could negatively impact the public's opinion or perception of the school as a whole.

School officials stated they would address these deficiencies to determine the appropriate corrective actions needed and adjust business practices if required. Campus D officials acknowledged the risk of reputational damage if a breach were to occur at an affiliate, and stated they would continue to work with their affiliates to ensure they achieve compliance, and have the affiliates annually provide an attestation of compliance to the school.

Preparing Self-Assessment Questionnaires

During the course of our audit, we found the SAQs from various school departments were either inaccurate or incomplete or had not been completed at all. SAQs are used by entities to assess their overall compliance with PCI DSS. Entities that accept credit card payments are required to fully complete their appropriate SAQ version. The completed SAQ is the school's attestation to full compliance with PCI DSS and can help identify those areas where elements of a PCI requirement have not been met fully.

During our site visits, we found SAQs that: had requirement questions unanswered; had requirements noted as "Not Applicable" (although they applied to the school environment being assessed); and lacked attestation responses in the PCI Validation portion of the form. Furthermore, one school (Campus E) has never completed and submitted a SAQ to its acquiring bank (the bank that processes credit card payments on behalf of the school).

In response to our preliminary findings, school officials generally noted the errors identified in the submitted SAQs were internal oversights and would be corrected. In addition, officials at Campus E noted they would contract with a QSA to assist in the process.

Ensuring a school or individual department has completed the proper SAQ version is critical, as incorrect or incomplete submissions could increase the risk of compromise or breach of credit card data. SAQs that are incorrect or incomplete could potentially allow systems' compliance deficiencies to go unaddressed or improper technical or operational controls to be applied to PCI system components, thus increasing the risk of exposure to breach.

Handling Paper Cardholder Data

Multiple PCI DSS requirements address how to properly handle cardholder data captured on hard-copy documents. This includes, but is not limited to, limiting the storage and retention time of credit card data to that which is required for business purposes, prohibiting the storage of sensitive authentication data after a transaction has occurred, masking or redacting the primary account number so that it is unreadable anywhere it is stored, limiting access to credit card data to only those individuals whose job responsibilities require access, and ensuring the secure destruction of those hard-copy documents containing cardholder data.

At two schools, Campuses B and F, we identified PCI DSS deficiencies regarding handling access to hard-copy documents, increasing the risk of unauthorized access to credit card data. Specifically, we observed:

- Improper storage at Campus F
  - Documents containing cardholder data were stored in a shared office location accessible to staff who did not have a direct business need for the data.
  - Hard-copy documents were kept after the transaction was processed and beyond the period of business need. This included transactions that were processed by staff several months prior to our site visit.

- Unsecure destruction of cardholder data at Campus B
  - Instead of being shredded, documents containing credit card data were torn in half and placed in a box below the counter.
  - One department did not have a shredder in the office, requiring staff to bring the hard-copy cardholder data to an adjacent building for shredding after processing the transactions.

As a result of our findings, staff at Campus F destroyed dated cardholder data during our visit. Further, Campus F officials stated they will lock the file drawer within the safe to prevent access by individuals not trained in PCI requirements, review business practices of retaining cardholder data, and ensure all departments follow the school's confidential paper destruction schedule. Officials at Campus B stated that their Financial Services staff will institute unannounced observation reviews of credit card processing departments on a regular basis, and share findings with Chief Financial Officers to develop action plans.

Following PCI DSS requirements regarding the proper handling, storage, and destruction of all hard-copy documents containing cardholder data is essential to minimize the potential risk of data exposure or compromise. Appropriate controls should be well documented in all policies and procedures in use at the schools, to be followed by those staff responsible for handling sensitive credit card data.

Guidance and Monitoring From System Administration

System Administration requires all schools to comply with PCI DSS, and has provided schools with some guidance on the protection of confidential data, including credit card information. For example, System Administration:

- Issued an Information Security Procedure and a SUNY Records Retention and Disposition Policy, which together detail specific protocols for the safeguarding of all sensitive information;
- Created a Security Operations Center (SOC) offering vulnerability scanning and penetration testing services to participating schools;
- Developed an Enterprise Risk Management Policy and Program in June 2015, tasked with identifying, assessing, and managing risk, including PCI compliance; and
- Provided schools with information security self-assessment questionnaires to help identify aspects of their operations that may require enhancement to their PCI DSS compliance.

However, we found areas where this guidance could be further developed to better assist schools in meeting PCI DSS compliance. For example, in its 2008 Guidelines, System Administration requires all State-operated schools to develop internal policies for the protection and security of sensitive data as well as establish administrative, technical, and physical safeguards to ensure the security of the data. However, although the document references PCI DSS, it does not provide any substantive insight into the required controls and best practices for implementation. Furthermore, System Administration's monitoring of schools' PCI compliance was limited. In particular, System Administration did not routinely perform information security audits, including PCI reviews, at

the various schools. At the time of our fieldwork, there had only been five information security audits, which addressed PCI standards, in the past six years. None of the schools we visited had received an audit.

The self-assessment process, which System Administration recently renewed in 2015 (and was previously performed in 2012), includes a questionnaire in which schools answer weighted questions regarding the information security management controls they have implemented. Although there are similarities between the technical controls reviewed in the self-assessment questionnaire and those required by PCI DSS, the System Administration questionnaire is not PCI focused. Thus, a high score on this assessment does not ensure sufficient PCI DSS compliance. Furthermore, the questionnaire does not include an assessment of operational controls for handling, processing, and storing cardholder data, which the PCI DSS otherwise requires.

We also found that System Administration's contract templates for affiliates, which most schools use as the basis for their contractual agreements, do not address PCI compliance and do not include provisions requiring affiliates to meet PCI DSS requirements. Nevertheless, because affiliates have access to schools' systems for credit card processing purposes, they are required to be PCI compliant. Inclusion of a PCI DSS provision in the contract templates would provide System Administration with an added measure of control over the SUNY network of data systems.

In response to our preliminary findings, System Administration officials noted they have taken a number of actions to help ensure confidential data (including credit card information) at the schools is secure, as previously detailed. System Administration stated they will continue to utilize the published PCI DSS requirements as guidance in presentations to inter-campus business professional organizations, conduct audits as risk assessments indicate, and be a resource to campuses that need assistance with implementing the Standards.

Further, System Administration noted that, although the contract templates do not include language for PCI DSS compliance, they do include information on an affiliate establishing a security program and the need to secure confidential data, which includes credit card information. System Administration also noted the SUNY Counsel's Office is presently considering revisions to contracts to include standard language related to PCI DSS.

Recommendations

To SUNY Schools visited:

1. Implement the recommendations contained in the detailed preliminary reports.

To System Administration:

2. Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all SUNY colleges.

3. Revise contract templates for affiliates to address PCI DSS regulations and require affiliates' compliance.

Audit Scope and Methodology

The objectives of our audit were to determine whether selected SUNY schools are in compliance with PCI standards and whether SUNY has provided sufficient guidance to the SUNY schools regarding PCI compliance. The audit covers the period August 25, 2015 to March 22, 2016.

To accomplish our objectives and assess related internal controls, we interviewed SUNY System Administration officials, including the Chief Information Officer, Information Security Officer, and internal audit officials as well as officials at each school to gain an understanding of the guidance given to SUNY schools and the PCI controls in place at each school visited. During our survey work, we administered a survey to a population of 30 entities, which included all 29 four-year SUNY schools as well as SUNY System Administration to determine if they accept credit cards, the method of acceptance, vendors used, and PCI compliance information. Based on the survey responses, the audit team selected a judgmental sample of six schools, including a variety of campus types, sizes, and locations. We conducted site visits and interviewed pertinent officials at each school to obtain an understanding of how credit cards are processed. In addition, we obtained and reviewed policies, procedures, and relevant documentation at each school, and witnessed how cards were actually processed by various departments.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to System Administration officials for their review and formal comment. Their comments were considered in preparing this report and are attached in

their entirety at the end of it. Officials generally agreed with our recommendations and indicated that steps are being taken to implement them. Additionally, we have omitted the names of the individual campuses from this final report at the request of System Administration.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Chancellor of the State University of New York shall report to the Governor, State Comptroller, and leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Contributors to This Report

John F. Buyce, CPA, CIA, CFE, CGFM, Audit Director
Brian Reilly, CFE, CGFM, Audit Manager
Nadine Morrell, CIA, CISM, CGAP, Audit Supervisor
Jared Hoffman, OSCP, GPEN, GWAPT, Information Technology Specialist
Holly Thornton, CFE, Examiner-in-Charge
Barbara Barfield, Senior Examiner
Peter Carroll, Senior Examiner
Chris Herald, Senior Examiner
Rachael Hurd, Senior Examiner
Anne Marie Miller, Senior Examiner
Sally Perry, Senior Examiner
Mary McCoy, Senior Editor

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

SUNY The State University of New York

Office of the
Chief Financial Officer

State University Plaza
Albany, New York 12246

www.suny.edu

May 25, 2016

John Buyce, CPA
Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street - 11th Floor
Albany, NY 12236-0001

Dear Mr. Buyce:

In accordance with Section 170 of Executive Law, we are providing our comments to the Office of the State Comptroller's (OSC) Draft Report, State University of New York (SUNY) Compliance with Payment Card Industry Standards (Draft Report). SUNY is committed to ensuring all of its campuses have appropriate controls and processes in place to secure our data and systems, and to effectively and securely process payments.

The report states that OSC identified multiple areas where significant improvements are needed to more fully address and meet the Payment Card Industry (PCI) requirements. To present a fair and balanced report, OSC should acknowledge that there are over 200 PCI requirements, many of which are complex; and furthermore, that the SUNY campuses audited by OSC have adequately addressed the majority of the standards.

SUNY has always used OSC's reports to improve our controls and processes, and to minimize risk. We appreciate your willingness to work with us to minimize the likelihood that information provided in the audit report does not compromise the security of sensitive data maintained by our campuses, a practice that is consistent with the policies of the Government Accountability Office (GAO).

Due to the sensitive nature of the topic, we are not providing a detailed response to the information cited in the report but would be glad to meet to discuss our action steps. However, we can state that our campuses have addressed, or are developing plans to address, the improvement opportunities identified by OSC. Our campuses continue to engage experts in the field to help ensure compliance with PCI requirements; this includes consideration for affiliates and related entities. These efforts require vertical integration, input, and cooperation from both operational and service units, with an attention to hardware, software, and controls. SUNY also recognizes that the consortium that mandates PCI requirements continues to update its criteria, and responding to these changes is challenging, but necessary.

The report notes that System Administration has not provided any additional insights into the required controls for PCI. This statement is not accurate in that System Administration has provided information and insights related to the requirements. However, SUNY System Administration has not reproduced or recreated the 200 plus PCI requirements as additional guidance to campuses in their compliance efforts. The detail and categorization of the PCI requirements, as issued, provides appropriate guidance to assist campuses in their efforts to address the requirements. We would further note that OSC has not issued any guidance on the PCI requirements for the multitude of State agencies that process credit card payments.

Responses to the Recommendations in the Draft Report

OSC issued three recommendations. Each of the three recommendations and our response follows:

To SUNY Schools visited:

1. *Implement the recommendations contained in the detailed preliminary reports.*

   The campuses visited during the course of the OSC audit have reviewed the findings and are addressing them, as appropriate. As previously noted, some campuses have engaged external PCI consultants several years ago, and all campuses are progressing and/or have completed initiatives to comply with PCI requirements.

To System Administration:

2. *Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all SUNY colleges.*

   Information security and compliance with PCI requirements is critical. As such, each SUNY campus has an information technology unit, which includes an information security officer. As OSC noted in the preliminary report, System Administration works with our campuses to enhance information security through a variety of support mechanisms including:

   - Our Security Operations Center offers vulnerability scanning and penetration testing services to subscribed campuses.
   - The Self-Assessment for Information Security Management questionnaire targets critical security controls, including some that relate to PCI requirements. The questionnaire is revised periodically and incorporates criteria directly applicable to the PCI requirements.
   - SUNY Procedure 6608 provides guidelines and standards for information security controls, including those addressing PCI requirements.
   - SUNY Enterprise Risk Management has identified PCI as a key risk, and assessments and evaluations are planned. We expect this process to result in system-wide benefits.
   - SUNY's Office of the University Auditor (OUA) conducts audits based on risk assessments; given the vast SUNY audit universe, the OUA has successfully completed five information security audits that included PCI standards, in the past six years.
   - SUNY OUA will share with campus business officers the results of this audit so that all SUNY campuses can benefit from the audit as they individually address PCI standards.

3. *Revise contract templates for affiliates to address PCI DSS regulations and require affiliates' compliance.*

   SUNY System Legal Counsel is addressing this recommendation and has enhanced the language in the affiliate contract templates for SUNY campus-related entities (e.g., foundations, auxiliary service corporations, etc.). They will make available these and all updated templates to campus procurement officers and other interested parties to ensure affiliates, as well as vendors, comply with PCI standards.

SUNY has a responsibility to its constituents, sponsors and customers to protect their confidential information. As such, SUNY appreciates that campus names and detailed findings will not be included in the final audit report. However, SUNY believes that citing information security weaknesses at any level in a public report could compromise our shared goal of strengthening data security. SUNY respectfully requests that in future information security audits, OSC return to its past practice of using two reports – one with detailed findings and recommendations for SUNY's internal use and one for the public with a high level summary of the audit. This is consistent with the approach used by the Office of Inspector General of the United States, Government Accountability Office (GAO), the government audit standards setting body in the country.

Thank you for the work your team has done.

Sincerely,

Eileen McLoughlin
Senior Vice Chancellor for Finance and
Chief Financial Officer

Copy: Chancellor Zimpher
Provost Cartwright
Mr. Abbott
Ms. Hengsterman
Ms. Labate
Ms. Liapis
Mr. Powalyk
Ms. Vattimo