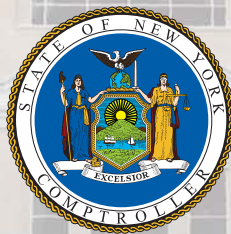




State Education Department

Security Over Online Registration Renewal and Teacher Certification

Report 2008-S-154



Thomas P. DiNapoli

Table of Contents

	Page
Authority Letter	5
Executive Summary	7
Introduction.....	9
Background	9
Audit Scope and Methodology	10
Authority.....	11
Reporting Requirements	11
Contributors to the Report	11
Audit Findings and Recommendation	13
Security Management.....	13
Recommendation.....	15
Agency Comments	17
State Comptroller's Comments	19

State of New York Office of the State Comptroller

Division of State Government Accountability

February 10, 2010

Mr. David Steiner
Commissioner
New York State Education Department
State Education Building - Rm. 111
89 Washington Avenue
Albany, NY 12234

Dear Commissioner Steiner:

Following is our report of Security Over Online Registration Renewal and Teacher Certification. Executive management took little action to ensure the Department met Payment Card Standards. By not complying with Payment Card Standards, the Department may be subject to data being improperly accessed and stolen. Significant fines could also be levied by the credit card vendors (e.g. VISA, MasterCard, etc.).

We urge you and your managers to act immediately on the report's recommendation and make the needed changes.

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*



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

Audit Objectives

- Did Department managers guard against the various risks associated with improper access to the Registration Renewal and Teacher Certification applications?
- Did Department managers meet the various security requirements for these applications?

Audit Results - Summary

Department managers do not guard against the various risks related to improper access to the Registration Renewal and Teacher Certification applications. Further, Department managers have not met the various security requirements for these applications. Managers have also not devoted sufficient resources to develop and implement a plan to meet the requirements for protecting customer data. In fact, Department managers did not have an adequate security organization in place. The organization should include resources for identifying risks, classifying data, and ensuring procedures exist for adhering to both the Payment Card Standards and Security Policy.

Our report contains one recommendation to improve controls over the Department's Registration Renewal and Teacher Certification applications.

This report, dated February 10, 2010, is available on our web site at: <http://www.osc.state.ny.us>
Add or update your mailing list address by contacting us at: (518) 474-3271 or

Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Introduction

Background

The State Education Department (Department) governs 48 licensed professions. It is responsible for licensing nearly 750,000 individuals and more than 30,000 professional business entities. The Department's Office of the Professions (Office) provides a number of services to the public and the professions such as processing forms, reviewing qualifications, and issuing credentials for various professions. The Office's Registration Renewal web-based application has been available since September 2007. It enables those who have licenses in certain professions, who are in the final five months of their current registration period or no more than four months past the expiration of their last valid registration period, to perform the following tasks online:

- Complete a registration renewal application,
- Request an optional Professional Photo ID Card and pay with a credit card,
- Choose to become inactive in the new registration period, and
- Change their address.

The Department also has a web-based application used by its Office of Teaching Initiatives called TEACH (Teacher Certification), which allows individuals to apply online for, and check the status of, teacher certifications (the focus of our review) and fingerprint clearances, among other services. Both applications were created by consultants and are maintained by the Department's Information Technology Services Application Development Unit (Application Development Unit).

Department managers must comply with the New York State Office of Cyber Security and Critical Infrastructure Coordination's (CSCIC) Cyber Security Policy (Security Policy) which defines a set of minimum information security requirements that all State entities must meet related to securing systems and data. For example, the Security Policy indicates that entities should classify data based on its confidentiality and availability. The Security Policy also requires that each State entity establish a framework to initiate and control its information security.

In addition, Department managers are required to adhere to Payment Card Industry Data Security Standards (Payment Card Standards) which were developed by members of the payment card industry such as Visa and

Master Card in 2006. The Payment Card Standards are a set of information security requirements that apply to all entities that process, transmit, or store cardholder data. They include requirements for security management, information security policies and procedures, network architecture, software design, and other critical measures to help organizations protect customer account data. Entities that fail to comply with Payment Card Standards could be subject to significant fines depending on the incident of non-compliance.

**Audit
Scope and
Methodology**

We audited selected aspects of the security controls in place over the Registration Renewal and Teacher Certification applications for the period October 17, 2008 through May 18, 2009. Our objectives were to determine whether Department managers: (1) guard against the various risks associated with improper access to the Registration Renewal and Teacher Certification applications and (2) meet the various security requirements for these applications.

We reviewed policies and procedures that we deemed important to the control and maintenance of application security. We interviewed agency technical staff responsible for controlling web application security and operations. We also examined records and reports pertinent to our audit scope. We tested security controls by determining whether there is a risk someone could gain improper access to the data maintained by the applications. In performing these assessments, we used various tools and techniques to pro actively identify application weaknesses and to determine how these weaknesses could be exploited. Our testing included scanning for weaknesses on specific servers and network devices, and more in-depth testing where we deemed it appropriate. Testing for web application weaknesses was performed on the Teacher Certification application only; however scanning for weaknesses was done on all devices related to the Teacher Certification and Registration Renewal applications. All scans had all dangerous tests turned off. Further testing is defined throughout this document. We also consulted with a Certified Payment Card Security Assessor to confirm the implementation of technology and processes for complying with the Payment Card Standards.

We did our performance audit according to 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 done according 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.

**Reporting
Requirements**

We provided a draft copy of this report to Department officials for their review and comment. We considered their comments in preparing this report. Department officials agree with our recommendation, but disagree with some of the findings which relate to compliance with Payment Card Standards. Officials believe that our criteria conflicts with advice they have received from other reputable sources. Regardless of this conflict, our report clearly shows Department managers are not meeting basic compliance requirements such as completing annual questionnaires and completing code reviews or installing necessary application firewalls.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of Education shall report to the Governor, the State Comptroller, and the 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 the Report**

Major contributors to this report include David R. Hancox, Brian Reilly, Nadine Morrell, Mark Ren, Corey Harrell, Jennifer Van Tassel, and Sue Gold.

Audit Findings and Recommendation

Security Management

The Department is required to identify and manage risks to its data. It is also required to adhere to policies and regulations such as the Payment Card Standards and Security Policy. We reviewed the Department's procedures relating to data security for the Registration Renewal and Teacher Certification applications. Department managers did not have an adequate security structure in place. This structure should include identifying risks, classifying data and procedures for adhering to both the Payment Card Standards and Security Policy.

Further, executive management devoted insufficient resources to developing and implementing a plan to meet Payment Card Standards, and no guidance was provided to the staff charged with ensuring the Department met applicable standards for handling credit card transactions. We also found that the Chief Information Officer assigned the position of Information Security Officer but did not give the person the authority to assign duties to other staff. The Information Security Officer has not been provided the resources necessary to complete all the functions required of an Information Security Officer by the Security Policy, including proper data classification.

Payment Card Standards

The information security requirements outlined in the Payment Card Standards apply to all system components that are included in or connected to the cardholder data environment (e.g., network components, servers and applications).

We found Department managers did not meet all Payment Card Standards requirements. For example, as of December 31, 2008, the Department should have completed two annual self-assessment questionnaires. However, neither of them was completed. In addition, Department managers did not adequately complete code reviews or install an application layer firewall, as required. Nor did they have the required quarterly scans done on network devices.

Department technology managers have had an agreement with CSCIC since November 2007 to scan for weaknesses on certain network devices on a monthly basis. However, we found that most devices involved in the processing of credit card payments have not been scanned, as required. We conducted our own scans on the servers and other devices that support the Registration Renewal and Teacher Certification applications. We found that

four of the eight network devices scanned had weaknesses that would cause them to fail a Payment Card Standards security test.

In addition, in March 2009, we scanned the Teacher Certification application. We found weaknesses that may allow unauthorized persons to access server setup data, modify web pages, cause a denial of service, or perform other harmful actions. Department Application Development Unit staff were not aware of these weaknesses and were not aware of the risks linked with some of their settings. These staff, along with the Information Security Officer also could not explain to us how credit card information flowed through their system when payments were authorized. We, along with a Certified Payment Card Security Assessor, had to re-create the steps to determine how the credit card information was processed so we could perform the appropriate testing.

These issues occurred because executive management took little action to ensure they met Payment Card Standards. For example, executive management devoted insufficient resources to developing and implementing a plan to meet Payment Card Standards. Also, no guidance was provided to the staff charged with ensuring the Department met applicable standards for handling credit card transactions. Department management assumed that certain Payment Card Standards did not apply to the Department and that sensitive customer data was secure without knowing their own systems. In response to our findings, Department officials indicated that they have recently sought guidance from another State agency on how to comply with Payment Card Standards.

By not complying with Payment Card Standards, the Department may be subject to various consequences such as data being improperly accessed and stolen. In addition, the Department could be subject to significant fines.

In response to our findings, Department officials stated CSCIC will continue to scan on a monthly basis the externally accessible network devices that support the Registration Renewal and Teacher Certification applications. They also said they had taken steps to address several of the weaknesses we found during our scanning. Department officials state they do not have the needed resources to scan all of the network devices that support the Registration Renewal and Teacher Certification applications. By not doing so, weaknesses could exist on these devices that Department managers may not be aware of and, therefore, the risk of improper access increases.

Security Policy - Data Classification

The Security Policy indicates that all agency information should be classified and managed based on its confidentiality, integrity and availability. Data

classification is a critical step that allows organizations to better understand the information that they actually have and then apply needed security measures to ensure sensitive information is protected appropriately. The Department's own procedures define three categories of data: public, restricted, and confidential. During the course of our audit, Department officials stated that data owners have been assigned, data has been classified, and controls have been implemented based on these classifications. However, we were provided with no evidence that data was classified in either the Registration Renewal or Teacher Certification applications.

In response to our preliminary audit findings, the Department did provide a data classification for Teacher Certification. Department officials stated that all data within Teacher Certification is public with the exception of 12 fields. However, we determined that not all of the data was classified appropriately. We believe there are additional fields contained within the database that may be sensitive, including data related to criminal background checks, child abuse, and child support. In reviewing the Department's security management organization, we found that the Chief Information Officer assigned the position of Information Security Officer but did not give the person the authority to assign duties to other staff. As a result, the Information Security Officer has not been provided the resources necessary to complete all the functions required of an Information Security Officer by the Security Policy, including proper data classification.

The Registration Renewal and Teacher Certification applications are supported by a database which contains various forms of sensitive and personally identifiable information. Without classifying the data residing on its network, management has no assurance that they are adequately protecting all of the Department's customer data.

Recommendation

1. Department managers should provide proper security over the sensitive data in the Registration Renewal and Teacher Certification applications. This includes providing adequate oversight and guidance to implement the necessary controls and procedures to address the findings noted in this report.

Agency Comments



THE STATE EDUCATION DEPARTMENT / THE UNIVERSITY OF THE STATE OF NEW YORK / ALBANY, NY 12234

DEPUTY COMMISSIONER FOR OPERATIONS
AND MANAGEMENT SERVICES
Tel. (518) 474-2547
Fax (518) 473-2827
E-mail: tsavo@mail.nysed.gov

January 20, 2010

Mr. David R. Hancox
Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street
Albany, NY 12236

Dear Mr. Hancox:

The following is the New York State Education Department's (NYSED) response to the Office of the State Comptroller's draft audit report (2008-S-154) of the State Education Department: Security Over Online Registration Renewal and Teacher Certification.

General Comments

The NYSED takes its responsibility to protect data entrusted to us by staff and customers very seriously. We make every effort to ensure that our practices are in full compliance with industry standards and best practices. A prime example of our proactive effort is the request we made to your office to conduct this audit. Our hope was to learn where additional improvements could be made. In fact, scans conducted by the OSC audit team revealed some opportunities for improvement that were immediately implemented.

NYSED's applications do not store or retain any credit card information in servicing customers of our Professions Online Registration Renewal and Teacher Certification systems. On numerous occasions prior to and during this audit, the Department's Information Security Officer (ISO) worked with New York State and external advisory services to identify best practices for data security for these applications. Contrary to the findings, NYSED technical staff always followed the guidance of the ISO who was given full authority in matters of information security by the Chief Information Officer.

The Department has adequate resources in place to implement the controls required to meet PCI standards, to meet the requirements of the NYS Security Policy, and to properly protect the customers' data. NYSED management and security personnel have given close attention over a period of years to ensuring that appropriate security controls are in place during the development of the subject applications and subsequent to its development.

*See State Comptroller's Comments on page 19.

*
Comment
1

*
Comment
2

Standards for protecting credit card transactions (PCI Security Standards) have evolved from being considered best practices to required standards. However, the required level of compliance is still being assessed by NYSED as well as other state agencies. The auditors' interpretation of certain published standards for protecting credit card transactions conflicts with advice we have received from other sources including Gartner Technology Business Research (Gartner). Gartner and other sources agree that the PCI Security Standards Council segmentation requirement is not specific.

*
Comment
3

NYSED has a history of conducting security scans of its infrastructure. For example, we were one of the first agencies working with the State's security agency, The Office of Cyber Security & Critical Infrastructure Coordination (CSCIC), to perform monthly scans, and have been awarded special recognition among state agencies by CSCIC for the comprehensive approach taken on follow-up actions to quickly eliminate vulnerabilities and put best practices in place. CSCIC is expected to further upgrade its highly regarded scans so that they are certified by PCI.

Below is our response to the one recommendation.

Recommendation

- 1. Department managers should provide proper security over the sensitive data in the Registration Renewal and Teacher Certification applications. This includes providing adequate oversight and guidance to implement the necessary controls and procedures to address the findings noted in this report.*

We agree with this recommendation. NYSED is confident that it currently provides adequate and appropriate security over the sensitive data in the Registration Renewal and Teacher Certification applications. We disagree with the auditor's findings that relate to the recommended level of compliance with the PCI standards. However, we are confident that these applications are in compliance with a reasonable understanding of the PCI standards.

*
Comment
3

If you have any questions regarding this response, please contact Richard Melita, Director, Information Technology Services, at (518) 474-4640.

Sincerely,



Theresa E. Savo

c: Richard Melita
David Walsh
James Conway

*See State Comptroller's Comments on page 19.

State Comptroller's Comments

1. We do not state that the Department stores or retains credit card information. We simply state that, "The Payment Card Standards are a set of information security requirements that apply to all entities that process, transmit, or store cardholder data." The web-based applications we examined clearly process card holder data.
2. Contrary to the Department's comment, we found the Chief Information Officer did not give the Information Security Officer appropriate authority to fulfill her responsibilities. For example, the Information Security Officer could not assign duties to staff in the technical units.
3. We reviewed and analyzed the criteria as required by audit standards. In addition, we consulted with a Certified Payment Card Security Assessor to confirm the implementation of technology and processes for complying with Payment Card standards. The Assessor confirmed OSC's assessment of the Payment Card standards as they relate to the Department. Our audit report clearly shows that the Department does not meet all Payment Card standards. For example, they did not complete two years of the Payment Card questionnaires, and did not complete code reviews or install application layer firewalls.