THOMAS P. DiNAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 22, 2010

Mr. Robert E. Beloten
Chairman
NYS Workers' Compensation Board
20 Park Street
Albany, NY 12207

Re: Network Security Controls
Report 2009-S-49

Dear Chairman Beloten:

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, we audited selected aspects of the security controls in place over the New York State Workers' Compensation Board's computer network (Network). Our audit covered the period August 13, 2009 through February 16, 2010.

A. Background

The Workers' Compensation Board (Board) provides weekly cash payments and the cost of full medical treatment, including rehabilitation, for covered employees who become disabled as a result of a disease or injury connected with their employment. In administering this program, the Board receives and processes workers' claims for benefits, employers' reports of injury, and medical reports from physicians and other health care providers. The Board maintains personally identifiable information such as date of birth, social security numbers, and medical information.

The Board has established a security framework with a Chief Information Officer responsible for balancing security with technical and program issues. In addition, the Board has a Security Unit responsible for setting standards for information security. The Security Unit is managed by an Information Security Manager and an Information Security Officer. The Security Unit reports directly to the Chief Information Officer.

The Security Unit has established several policies for protecting their Network data and resources. In 2008, the Security Unit began a Security Remediation project to address critical security requirements. The Security Unit monitors the use of hardware, software, and data to ensure security standards are met, investigates breaches in security, and works with Board management and outside law enforcement to apprehend violators.

The Board must comply with New York State's Office of Cyber Security and Critical Infrastructure Coordination's Cyber Security Policy (Security Policy), which defines a minimum

set of security standards State entities must meet. One of these standards is managing the risk of security exposure or compromise within the entity's system.

B. Audit Scope, Objective and Methodology

We did our performance audit according to generally accepted government auditing standards. We audited selected aspects of the security controls in place over the Network for the period August 13, 2009 through February 16, 2010. The objective of our audit was to determine whether network security at the Board is sufficient to minimize the risks of unauthorized access to its data and resources.

We reviewed Board policies and procedures we deemed important to the control and maintenance of Network security. We interviewed agency technical staff responsible for Network 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 unauthorized access to the Network. These tests were performed on some, but not all, devices on the external and internal Network. In performing these assessments, we used various tools and techniques to identify Network weaknesses and to determine how these weaknesses could be exploited. Our testing included scanning for weaknesses on; specific servers, workstations, and web applications, and more in-depth testing of select servers and applications where we deemed it appropriate.

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.

C. Results of Audit

We found numerous critical weaknesses on the Board's Network which need to be corrected to ensure the Board's data and resources are not at risk. Board management has not taken fundamental steps to secure their Network, such as completing a risk assessment and data classification. Detailed results of our audit were provided to Board officials during our audit. The details of our findings and recommendations are not included here due to the sensitivity of the information and the potential risk associated with the release of such information. Board officials stated they have begun to make improvements.

Recommendation

Implement the specific recommendations for strengthening the Board's network security that were provided to Board officials during the audit.

We provided a draft copy of this report to Board officials for their review and comment. Their comments were considered in preparing this report and are included as Appendix A.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Chairman of the New York State Workers' Compensation Board 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 recommendation contained herein, and where the recommendation was not implemented, the reason therefor.

Major contributors to this report include Brian Reilly, Nadine Morrell, Claudia Christodoulou, Jennifer Van Tassel, Corey Harrell, Randy Rose, and Sue Gold.

We wish to thank the management and staff of the Workers' Compensation Board for the courtesy and cooperation extended to our auditors during this audit.

Yours truly,

David R. Hancox
Audit Director

cc: Tom Lukacs, Division of the Budget

DAVID A. PATERSON
GOVERNOR

STATE OF NEW YORK
WORKERS' COMPENSATION BOARD
20 PARK STREET
ALBANY, NEW YORK 12207
(518) 408-0469
(518) 486-3515 Fax

ROBERT E. BELOTEN
CHAIR

June 11, 2010

David R. Hancox
Audit Director
Office of the State Comptroller
110 State Street, 11th Floor
Albany, NY 12236

Re: Report 2009-S-49

Dear Mr. Hancox:

This letter is in response to Office of the State Comptroller's (OSC) Audit Findings and Recommendations Report, developed during the Network Security Controls audit conducted from August 13, 2009 through February 16, 2010.

The Board recognizes that the most critical vulnerabilities identified by OSC during the audit required immediate attention, and has taken appropriate action to address those vulnerabilities. An action plan was developed to address the remaining weaknesses identified in the Audit Findings and Recommendations Report. Steps have been taken to secure the Board's network, including the initiation of security projects such as a risk assessment and data classification. In addition, the Board will incorporate OSC's recommendations to ensure that these vulnerabilities are not repeated.

The Board's management team is committed to protecting the Board's network data and resources and complying with the NYS Office of Cyber Security & Critical Infrastructure Coordination's Security Policy.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Robert E. Beloten

Robert E. Beloten
Chair

cc: Uluss (Gus) Thompson, Deputy Director of Administration

Appendix A