

THOMAS P. DiNAPOLI  
STATE COMPTROLLER



110 STATE STREET  
ALBANY, NEW YORK 12236

STATE OF NEW YORK  
**OFFICE OF THE STATE COMPTROLLER**

July 8, 2010

Ms. Jamie Woodward  
Acting Commissioner  
Department of Taxation and Finance  
W. A. Harriman Campus, Building 9  
Albany, New York 12227

Re: Wireless Security Controls  
Report 2010-S-8

Dear Ms. Woodward:

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 wireless security controls in place at the New York State Department of Taxation and Finance. Our audit covered the period February 9, 2010 through April 16, 2010.

**A. Background**

The Department of Taxation and Finance (Department) administers the State's tax laws and serves as the State's general tax collection agency. The various taxes collected and administered by the Department include Corporation, Personal Income, Sales, and other miscellaneous taxes. Annually, the Department collects over \$52 billion in State tax revenue and over \$33 billion in local taxes on behalf of municipalities. The Department has a total workforce of almost 5,000 employees working in 13 offices and 5 other sites located throughout the State.

Department security policies are issued to all employees, consultants, contractors, external auditors and outside agents. Employees are reminded annually of their responsibility to adhere to the policies and are notified electronically of any policy changes. In addition, Department computer systems display a warning banner that indicates the computer system contains government information and is to be used only by authorized individuals. It also warns that actions on the system may be monitored and the unauthorized disclosure of information is subject to penalty.

The Department 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. The Security Policy requires State entities to perform a risk assessment before installing a wireless network or wireless access point and to obtain written approval from the entity's Information Security Officer.

## **B. Audit Scope, Objective and Methodology**

We audited selected aspects of the security controls in place over the network for the period February 9, 2010 through April 16, 2010. The objective of our audit was to determine if unauthorized access points are present on the Department's network which provides access to sensitive data.

We reviewed Department policies and procedures we deemed important to the control and maintenance of wireless security. We interviewed agency technical staff responsible for wireless security and operations. We also tested security controls by determining whether there were any unauthorized wireless access points at all Department locations. In performing these tests, we used various tools and techniques to identify unauthorized access points.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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 and do not affect our ability to conduct independent audits of program performance.

## **C. Results of Audit**

We did not locate any unauthorized wireless access points during our testing, but access points can easily be installed at any time and may allow an unauthorized person to get into the Department's network. The Information Technology Services staff does not perform any testing to ensure there are no unauthorized access points on its network. We recommend periodic, random testing be completed to ensure unauthorized wireless access points are not attached to the Department's network.

We found Department staff has taken measures to monitor known access points, including conducting a risk assessment and establishing a wireless access policy. The policy includes performing a risk assessment before installing a wireless network or wireless access point and obtaining written approval. In addition, according to Department officials, they have authentication requirements and encryption on their approved wireless networks.

**Recommendation**

*Complete periodic, random testing to detect unauthorized wireless access points at all Department offices.*

We provided a draft copy of this report to Department 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 Commissioner of the Department of Taxation and Finance 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 reasons therefor.

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

We wish to thank the management and staff of the Department of Taxation and Finance 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  
James Brunt, Internal Audit Director

This report, dated July 8, 2010, is available on our website 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, 11<sup>th</sup> Floor  
Albany, NY 12236



STATE OF NEW YORK  
DEPARTMENT OF TAXATION AND FINANCE  
W A HARRIMAN CAMPUS  
ALBANY, NY 12227

JAMIE WOODWARD  
ACTING COMMISSIONER

June 25, 2010

Mr. David R. Hancox  
Audit Director  
Office of the State Comptroller  
Division of State Government Accountability  
110 State Street, 11<sup>th</sup> Floor  
Albany, NY 12236

Dear Mr. Hancox:

Thank you for the opportunity to comment on your draft audit report (2010-S-8) "*Wireless Security Controls*." We are pleased that your auditors found no instances of unauthorized wireless access points at the 19 Department locations visited. Your draft audit report also recognized our security policies, practices and awareness training for wireless security. As your report pointed out, the Department needs to implement a formal program of testing for unauthorized wireless access points.

Following is our specific response to the recommendation:

**Recommendation:**

*Complete periodic, random testing to detect unauthorized wireless access points at all Department offices.*

**DTF Response:**

We agree. The Department's Office of Information Technology Services (OITS) has acquired the software used by the OSC auditors to detect unauthorized wireless access points and has developed a plan for periodic testing at the District Offices. OITS intends to begin testing in June 2010 and to test every location at least once a year.

Thank you for your suggestions to improve our operations.

Sincerely,

A handwritten signature in cursive script that reads "Jamie Woodward".

Jamie Woodward  
Acting Commissioner