

THOMAS P. DiNAPOLI
COMPTROLLER



110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

February 17, 2012

Ms. Patricia Hite
Acting Commissioner
Director, Classification and Compensation
NYS Department of Civil Service
Alfred E. Smith State Office Building
Albany, NY 12239

Re: Report 2011-S-7

Dear Ms. Hite:

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 over the New York State Department of Civil Service's computer network. Our audit covered the period February 8, 2011 through September 7, 2011.

Background

The Department of Civil Service is the central personnel agency for the State of New York and provides a variety of human resource services. Over the last six years, the Department has implemented a strategic initiative to use web-based applications to support the agency's mission and objectives. This initiative focuses on delivering customer service through e-government solutions.

The Department must comply with the New York State Office of Cyber Security's Information Security Policy (Security Policy), which defines a minimum set of security standards State entities must meet. One objective of the Security Policy is to manage the risk of security exposure or compromise within the entity's system. In addition, the Department has its own Information Security Policy that requires all Department information to be protected from unauthorized access.

Results of Audit

The Department's data and resources are at risk of unauthorized access, disclosure of sensitive data, and denial of service, in part because the Department has not evaluated the effectiveness of all of its security controls. Without this evaluation, the Department cannot be sure its controls adequately secure confidential data.

Detailed results of our tests were provided to Department 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. Department officials stated they have begun to make improvements.

Recommendation

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

Audit Scope, Objective and Methodology

We audited selected aspects of the security controls in place for the period February 8, 2011 through September 7, 2011. The objective of our audit was to determine whether confidential data at the Department of Civil Service was secure from unauthorized access.

In performing this assessment, we reviewed Department policies and procedures that we deemed important to the scope of our audit, and interviewed members of the Information Security Team, as well as other technical staff responsible for network security and operations. We also examined records and reports pertinent to our audit scope, and used various electronic tools and techniques to identify weaknesses and to determine how these weaknesses could be exploited. Our testing included evaluating the effectiveness of the Department's firewall and scanning its public website, one of its internal web applications, and specific servers associated with this and other applications, for known weaknesses.

We conducted our 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 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.

We provided a draft copy of this report to Department officials and are included as Appendix A. Department officials agreed with our recommendations and have already taken steps to address our findings.

Within 90 days of the final release of this report, Department officials shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising

the steps they have taken to implement our report recommendations, and where recommendations were not implemented, the reasons therefor.

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

We wish to thank the management and staff of the Department of Civil Service for their courtesy and cooperation extended to our auditors during this audit.

Yours truly,

A handwritten signature in black ink, appearing to read "John L. Buyce". The signature is fluid and cursive, with a prominent initial "J" and a long, sweeping underline.

John Buyce, CPA, CIA, CGFM
Audit Director

cc: Thomas Lukacs, Division of the Budget
Frank Slade, Department of Civil Service



ANDREW M. CUOMO
GOVERNOR

STATE OF NEW YORK
DEPARTMENT OF CIVIL SERVICE
ALFRED E. SMITH STATE OFFICE BUILDING
ALBANY, NEW YORK 12239
www.cs.ny.gov

February 3, 2012

Mr. John Buyce
Audit Director
Office of the State Comptroller
110 State Street
Albany, New York 12236

Re: Report 2011-S-7

Dear Mr. Buyce,

The Department of Civil Service has reviewed the findings and recommendations in the Office of the State Comptroller's (OSC) draft report on the Department's selected general controls over data security and substantially agrees with the recommendations presented in the report. The Department is committed to ensuring the integrity and security of its information technology environment and the report provides valuable recommendations for the Department to further strengthen its information security and assurance efforts.

The Department appreciates the efforts of the OSC auditors in assisting to strengthen our network security and information security program.

Sincerely,

A handwritten signature in cursive script that reads "Patricia A. Hite".

Patricia A. Hite
Acting Commissioner

cc: Deirdre Taylor, Deputy Commissioner
Frank Slade, Director of Information Technology Services
Thomas Lukacs, Division of Budget