ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 3, 2003

Mr. Randy A. Daniels
Secretary of State
Department of State
41 State Street
Albany, NY 12231-0001

Re: Report 2003-F-12

Dear Mr. Daniels:

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, we have reviewed the actions taken by officials of the Department of State (Department) as of June 2, 2003 to implement the recommendations contained in our audit report, *Computer Network Security Controls* (Report 2001-S-47). Our report, which was issued on June 13, 2002, assessed the adequacy of controls over the Department's computer network.

Background

The Department performs a number of important duties involving the protection of public safety by managing fire prevention programs, building and energy codes programs, corporation and uniform commercial code programs, and ombudsman services. The Department also licenses a number of professions and occupations, including notaries, the real estate and appearance enhancement industries, and various security services. In addition, the Department administers community development programs and local government service activities, and provides administrative support for several offices, including the State Ethics Commission, the State Athletic Commission, and the Committee on Open Government.

The Department's computerized information systems support the execution of these important duties. The Department's customers can obtain certain licensing applications, publications and information on-line, and can also access databases to check the registry of Department licensees and business entities. To enable its customers to transact more business quickly and easily, at the time of our audit, the Department was in the process of developing on-line filing, license renewal, and information reporting capabilities.

To develop these capabilities, the Department is moving from a mainframe-based environment, where all applications reside on a mainframe computer maintained by the New York State Office for Technology, to a server-based environment, in which some mission-critical applications (such as Fire Incident Reporting, Uniform Commercial Code filings, and renewals of Real Estate Licenses) will reside on site and will be administered by the Department.

At the time of our audit fieldwork, the Department's computer system network comprised more than 50 servers and had approximately 800 users. The Department's Bureau of Systems Management is responsible for system development, technical support, network and user support, and network security.

Summary Conclusions

In our prior audit, we identified the need for significant improvements in the Department's information systems security controls to better protect the integrity of computerized information systems and the confidentiality of electronic data. We also found that the Department's primary focus had been on implementing new applications without giving sufficient consideration to or providing adequate resources for security controls. Additionally, Department officials refused to fully cooperate with our audit. Hence, we were unable to undertake all of our planned audit tests of the security of the Department's computer system network.

In our follow-up review, we found that Department officials have made progress in implementing the audit recommendations. For three of the six recommendations, the Department hired consultants to draft policies and procedures to address our audit recommendations. At the time of our review, the consultant's work was still in progress. With respect to the remaining three recommendations, the Department either hired a contractor or attempted to address the recommendations directly.

Summary of Status of Prior Audit Recommendations

Department officials have partially implemented all six of the prior audit recommendations.

Follow-up Observations

Recommendation 1

Complete a comprehensive security policy in a timely manner.

Status – Partially Implemented

Agency Action – In April 2003, the NYS Office of Cyber Security & Critical Infrastructure Coordination issued a new baseline security policy. According to Department officials, implementation of a comprehensive security policy in accordance with this recommendation was delayed in order to satisfy all of the requirements imposed on the Department by the new baseline security policy. At the time of our follow-up review, Department officials

stated that approximately 20 percent of the Department's comprehensive security policy still needed to be implemented.

Recommendation 2

Perform a risk assessment of the entire network, including an assessment of assets, vulnerabilities of those assets, the probability of exploitation, the impact of exploitation and a viable means of protection.

Status – Partially Implemented

Agency Action – In December 2002, the Department went out to bid for a Disaster Recovery and Business Continuity Planning Project. The project consists of several deliverables, the second deliverable of which pertains to risk assessment. Work on the risk assessment deliverable began on March 4, 2003 and is scheduled to be completed on June 27, 2003.

Recommendation 3

Designate a full-time ISO with the appropriate authority and independence to perform the duties outlined in the New York State Office for Technology's policy, such as providing additional training or other resources for security awareness and understanding the security policies and procedures.

Status – Partially Implemented

Agency Action – The Information Security Officer (ISO) position has been approved by the Department of Civil Service, and the Department is currently working towards filling this position. The Director of Internal Audit is currently the interim ISO. However, there is potential for a conflict of interest between the two positions. The Office of Internal Audit is responsible for overseeing the effectiveness and efficiency of agency operations by conducting internal audits, including audits related to information security. Thus, the Office of Internal Audit is not independent of any audits addressing information security issues. According to Department officials, they recognize the issue and are considering having reviews of the information security function conducted by an outside entity that would report directly to executive management.

Recommendation 4

Develop Disaster Recovery and Business Continuity Plans for use in the event of a natural or man-made disaster that might disrupt business processes. Formally document, execute and periodically test the Plans.

Status – Partially Implemented

Agency Action – As noted above, in December 2002, the Department went out to bid for a Disaster Recovery and Business Continuity Planning Project. The fourth deliverable on the project pertains to Disaster Recovery and Business Continuity Planning. Work on the Disaster

Recovery and Business Continuity Planning deliverable began on March 4, 2003 and is scheduled to be completed on August 26, 2003.

Recommendation 5

Improve physical security controls over information systems by addressing the weaknesses identified by this audit.

Status – Partially Implemented

Agency Action – We toured the Department's various computer rooms and found that the Department has made some progress in improving physical security controls. We provided Department officials with the details of the remaining weaknesses we identified during the course of this review.

Recommendation 6

Take corrective actions to address the weaknesses in logical controls on the servers as identified by this audit.

Status – Partially Implemented

Agency Action – We reviewed the baseline security configurations of two out of ten previously tested servers and identified that weaknesses in the logical controls on these two servers still existed. Since these controls are designed to prevent or detect unauthorized access to a computer network, we provided Department officials with the details of our findings during the course of this review.

Department officials identified the steps they had taken, and continue to take, to address our previous recommendation related to the logical controls on the servers. Once completed, these steps should allow the Department to fully implement this recommendation.

Major contributors to this report were Walter Irving, Nadine Morrell and Simon Prazak.

We would appreciate your response to this report within 30 days, indicating any actions planned or taken to address any unresolved matters discussed in this report. We also thank Department management and staff for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Kevin M. McClune
Audit Director

cc: Deirdre A. Taylor