

THOMAS P. DINAPOLI  
COMPTROLLER



110 STATE STREET  
ALBANY, NEW YORK 12236

STATE OF NEW YORK  
OFFICE OF THE STATE COMPTROLLER

August 29, 2007

Mr. Brian Fischer  
Commissioner  
New York State Department of Correctional Services  
Harriman State Office Building Campus - Bldg 2  
1220 Washington Ave  
Albany, New York 12226-2050

Re: Report 2007-F-12

Dear Mr. Fischer:

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 followed up on the actions taken by officials of the Department of Correctional Services to implement the recommendations contained in our audit report, *Network Security Controls* (Report 2005-S-27).

**Background, Scope and Objectives**

The Department of Correctional Services (Department) has created a computer network (Network) to help manage the Department's population of approximately 63,500 inmates within its 69 state correctional facilities and the 850-bed Willard Drug Treatment Campus. The Network facilitates access to applications the Department uses to manage the inmate population. Department employees also use the Network to access the Internet and e-mail, as well as files on the internal network. The Department's Management Information Systems (MIS) Unit is responsible for managing the Network. This includes supporting all servers, providing network connectivity for business units and correctional facilities, and managing network devices.

New York State agencies are expected to comply with the requirements of the State's Cyber Security Policy, which was developed by the Office of Cyber Security and Critical Infrastructure Coordination. Each agency is expected to meet the specific security requirements described in the Policy, and to establish a framework for initiating and controlling the implementation of information security within the agency.

Our initial audit report, which was issued on June 5, 2006, examined selected aspects of the security controls in place over the Department's Network. The objective of our follow-up, which was conducted in accordance with generally accepted government auditing standards, was to assess

the extent of implementation as of July 12, 2007 of the recommendations included in our confidential report. Due to the sensitivity of the information and the potential risk associated with the release of such information, the details of the recommendations and their implementation status are not included in this report. However, we discussed the detailed results of our follow-up work with Department officials during the conduct of the follow-up.

### **Summary Conclusions**

Overall, we found that Department officials have taken preliminary actions to implement the recommendations contained in the confidential draft report. While Department management agrees with our audit recommendations and included several of them in its top information security priorities, we found much work still needs to be done to implement our recommendations. The Department needs to be more timely in taking corrective action or it will be vulnerable to significant risks to its network. Department officials agreed with our conclusions and indicated they will take additional actions to fully implement the recommendations.

Major contributors to this report were Nadine Morrell, Mark Ren, Eric Booker and Andrew White.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed during the course of our follow-up. We also thank Department management and staff for the courtesies and cooperation extended to our auditors during this process.

Very truly yours,

Brian Reilly  
Audit Manager

cc: Ms. Lisa Ng, Division of the Budget  
Ms. Debbie Coons, Department of Corrections