2002-0235-4T February 28, 2002

Ms. Cheryl Dennis, Assistant Sergeant-at-Arms
Office of the Sergeant-at-Arms
State House, Room 46
Boston, Massachusetts 02133

Dear Ms. Dennis:

From December 13, 2001 to December 28, 2001, we performed a review of selected information technology (IT)-related controls at the Office of the Sergeant-at-Arms. The purpose of the internal control review was to evaluate the appropriateness and adequacy of selected controls over and within the Sergeant-at-Arms IT-related environment. As a result of our review, we are issuing this management letter pertaining to internal control practices for your IT environment.

The Office of the Sergeant-at-Arms is organized under Chapter 3, Section 17 of the Massachusetts General Laws. The mission of the Sergeant-at-Arms is to provide security and maintain order for the General Court, specifically the House of Representatives and Senate chambers and hearing rooms. In conjunction with the Sergeant-at-Arms mission, the Office processes the payroll for the General Court's officers and pages and for the staff of the legislative document room. Other administrative functions include the purchase of subscriptions to newspapers and professional publications.

With respect to the scope of our IT-related control review, we reviewed selected general controls pertaining to physical security, environmental protection, and inventory controls over the microcomputer systems installed in the administrative office. In addition, we reviewed and evaluated security over personnel files in hardcopy form stored in the administrative office. Because our review indicated that the Sergeant-at-Arms' computer systems were connected to the Senate's network, we did not review control areas, such as system access security to automated systems, business continuity planning, and on-site and off-site storage of backup media that were within the jurisdiction of the Senate's Information Technology Division (ITD). Further, we did not review the formal IT-related policies and procedures regarding control areas within the Senate's jurisdiction. Our review included interviews with relevant managers, documentation reviews, inventory tests, and on-site observations.

As a result of our review, certain observations were made regarding the existing control environment that we would like to present to assist you in ensuring that adequate IT-related controls are in place. We observed the following internal control strengths.

- To help provide assurance that only authorized users can access the Sergeant-at-Arms automated systems, the Office requests authorization from the Senate's ITD that a user be granted access privileges, and assigned a logon ID and password.

The Senate's ITD is notified when an employee of the Sergeant-at-Arms terminates his or her position. According to prior Sergeant-at-Arms, the Senate's ITD grants users a logon ID and password. It is our understanding that passwords are changed every 60 days.

- To help ensure adequate physical access security to the Sergeant-at-Arms' offices, sufficient security procedures, such as identification of all visitors to the building, capital police patrols, burglar alarms, and locked doors were in place within the State House in which the Sergeant-at-Arms administrative office was located. We determined that microcomputer systems within the administrative office were secure. Further, our review indicated that personnel files stored in hardcopy form were also physically secure. At the time of our audit, the Sergeant-at-Arms controlled the distribution and return of keys for the six administrative staff. We found that access keys were stamped "do not duplicate." In addition, we found that the door to the administrative office was locked after normal business hours. According to the prior Sergeant-at-Arms, the Senate's Information Technology Division was responsible for formal policies and procedures regarding physical security.

- To maintain environmental protection controls within the Sergeant-at Arms administrative offices, we determined that automated systems were protected by controls such as fire alarms, sprinkler systems, and temperature controls. We determined that to help prevent the loss or corruption of data, surge protector devices were in place.

- We noted that the microcomputer systems were properly tagged with state identification numbers. The Sergeant-at-Arms had assigned responsibility for inventory control to a specific staff person. We determined that actual computers on hand were accurately listed on the inventory record.

This letter is intended solely for use by the Sergeant-at-Arms management in assessing controls regarding the IT environment and in facilitating corrective action where needed. If you determine that there are areas of IT-related controls that warrant further information, please contact us and we will have our IT Audit Division review the control issues with you.

We would like to express our appreciation for the courtesy extended by you and your staff during the review. Our staff enjoyed meeting and working with you and Mr. Michael J. Rea, Jr., Sergeant-at-Arms during our audit and appreciate your assistance. Should you need additional information regarding this management letter, we would be pleased to provide it.

Sincerely,

A. Joseph DeNucci
Auditor of the Commonwealth

cc: Mr. Richard Rossi, Director, Information Technology Division, State Senate
Ms. Margaret Rooney, Director, Legislative Data Processing, House of Representatives
Ms. Patricia Foley, Business Manager, House of Representatives