State of New York
Office of the State Comptroller
Division of Management Audit

CONTROLS RELATING TO LICENSED SOFTWARE AND COMPUTER VIRUSES AT SELECTED STATE AGENCIES

REPORT 96-S-51

H. Carl McCall

Comptroller

State of New York
Office of the State Comptroller

February 3, 1998

Division of Management Audit
Report 96-S-51

Mr. James G. Natoli
Chairperson
Governor's Task Force on Information
Resource Management
State Capitol
Albany, New York 12224

Mr. Richard Jackson
Commissioner
Department of Motor Vehicles
Empire State Plaza
Swan Street Building
Albany, New York 12228

Mr. Joseph J. Seymour
Commissioner
Office General Services
Tower Building 41st Floor
Albany, New York 12242

Barbara A. DeBuono, MD
Commissioner
Department of Health
Corning Tower
Empire State Plaza
Albany, New York 12237

Mr. Charles Gargano
Chairman
Empire State Development Corporation
633 Third Avenue
New York, New York 10017

Mr. Brian Wing
Commissioner
Department of Social Services
40 North Pearl Street
Albany, New York 12243

Mr. Joseph H. Boardman
Acting Commissioner
Department of Transportation
40 North Pearl Street
Albany, New York 12243

Ms. Elizabeth McCaul
Acting Superintendent
State Banking Department
2 Rector Street
New York, New York 10006

Mr. Neil D. Levin
Acting Superintendent
State Insurance Department
25 Beaver Street - 3rd Floor
New York, New York 10004

Dr. DeBuono, Ms. McCaul, and Messrs. Natoli, Jackson, Seymour, Gargano, Wing, Boardman, and Levin:

The following is our report addressing controls relating to licensed software and computer viruses at seven State agencies and a public benefit corporation.

This audit was done according to the State Comptroller's authority as set forth in Section 1, Article V of the State Constitution and Section 8, Article 2 of the State Finance Law. We list major contributors to this report in Appendix A.

Office of the State Comptroller
Division of Management Audit

Executive Summary

Controls Relating To Licensed Software And Computer Viruses At Selected State Agencies

Scope of Audit

New York State agencies, authorities and public benefit corporations collectively own more than 50,000 microcomputers as well as a considerable amount of computer software. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. The unlicensed use and replication of computer software is punishable by fines of up to $100,000 per violation in civil proceedings and $250,000 per violation in criminal proceedings. Microcomputers are also vulnerable to infection from computer viruses, which can be costly and time-consuming to eradicate, and can destroy or corrupt valuable information. The risk of infection from computer viruses has increased dramatically as people make greater use of computer programs obtained through the Internet and other sources. New York State has yet to develop guidelines for its agencies addressing the use of licensed software and protection against computer viruses. The Governor's Task Force on Information Resource Management would be the State entity responsible for developing such guidelines. (In August 1997, legislation formally changed the name of the Governor's Task Force on Information Resource Management to the New York State Office for Technology.)

We audited the procedures used by seven State agencies and a public benefit corporation (agencies) to prevent the use of unlicensed software and protect against computer viruses during the period July 1, 1994 through February 20, 1997. The eight agencies, which together own about 19,000 microcomputers, include the Banking Department, the Department of Health, the Department of Motor Vehicles, the Department of Social Services, the Department of Transportation, the Empire State Development Corporation, the Insurance Department, and the Office of General Services. Our audit addressed the following questions:

- Are the procedures used by the eight agencies to prevent the use of unlicensed software and protect against computer viruses adequate?

- Can the best of these procedures be incorporated in the statewide guidelines that may be developed by the Governor's Task Force on Information Resource Management?

Audit Observations and Conclusions

We found that, in some instances, the agencies have developed, or are developing, and follow a number of appropriate procedures. These procedures, collectively, could be considered "best practices" and could be of use to the Governor's Task Force on Information Resource Management in its development of statewide guidelines. However, significant improvements can still be made in other procedures at each of the eight individual agencies. Because of control weaknesses at these agencies, the agencies'

microcomputers are more likely to contain unlicensed software and computer viruses. In fact, when we tested 212 microcomputers at five of the agencies, we found that they contained a total of 246 unlicensed computer applications and three computer viruses. (See p.5)

According to the Gartner Group, Inc., an internationally recognized technology consulting firm, there are a number of practices that can help organizations prevent the use of unlicensed software and protect against computer viruses. For example, organizations can monitor employees' use of computer applications, periodically inventory the applications, conduct surprise audits of the software installed on microcomputers, use virus detection software, maintain a log of virus infections, and educate employees about the dangers of computer viruses and the need to avoid the use of unlicensed software. However, we found that many of these practices are either not used properly, or are not used at all, by the eight agencies addressed by our audit. (See pp.4-9)

We believe these control weaknesses can be attributed in part to a lack of statewide guidelines concerning the use of microcomputers. We also believe that upper management at these agencies has not adequately emphasized the importance of these controls, and note that the agencies have conducted few internal audits addressing microcomputer controls. (See p.6)

We tested 212 microcomputers at five of the agencies to determine whether the computers contained unlicensed software. We also tested 167 microcomputers at these same five agencies to determine whether the computers contained viruses. We found that the microcomputers contained a total of 246 unlicensed applications, including 109 games, which did not come bundled with the machine. We also found that virus detection software had been disabled on 44 of the microcomputers, and 3 microcomputers had been infected by computer viruses. If the agencies do not improve their controls for preventing virus infections, they risk losing important data and incurring large recovery costs as a result of virus infections. (See pp.6-9)

We recommend that the eight agencies improve their procedures relating to unlicensed software and computer viruses, and actively follow up to ensure that the procedures are implemented as intended. We also recommend that the Governor's Task Force on Information Resource Management consider incorporating into its statewide guidelines the best practices summarized in this report and in Exhibit A. (See pp.10-11)

Comments of the Governor's Task Force and Agencies' Officials

The Governor's Task Force and the agencies' officials generally agreed with the report's findings and recommendations. These officials state that they have either implemented the recommendations or currently have the proper controls in place.

Contents

Introduction

Background

New York State agencies, authorities and public benefit corporations collectively own more than 50,000 microcomputers as well as a considerable amount of related computer software. Since 1980, the Federal Copyright Act has protected computer software against unauthorized replication or other uses not sanctioned by the license accompanying the software. Each instance of software copyright infringement is punishable in civil actions by a fine of up to $100,000. The penalties in criminal actions include fines up to $250,000 and/or five years imprisonment. Nevertheless, according to the Business Software alliance, approximately 35 percent of the business software used in the United States is unlicensed.

The proliferation of microcomputers has dramatically increased the risk of computer viruses because many users may share or exchange a variety of programs from various sources. The use of the Internet to send and receive software, and the availability of shareware and freeware, also increase the risk of getting a virus. A computer virus can be very costly and time-consuming to eradicate and can destroy or corrupt valuable information. According to the National Computer Security Association's (NCSA) 1996 Computer Virus Prevalence Survey, the chances of encountering a virus in 1996 were five to ten times higher than in early 1995. The NCSA's poll of 300 companies and government agencies concluded that for every 1,000 machines used by an organization, the organization can expect to get a virus 120 times annually. According to the poll, the organizations needed, on average, over forty hours, or about one work week, to recover completely from a virus.

In 1996, the Governor's Task Force on Information Resource Management (Governor's Task Force)[1] was created to improve how State agencies use technology to manage information. Among the goals of the Governor's Task Force are to establish statewide policies and practices for new technologies, design new ways to secure and protect information, and identify the best practices among State agencies for possible statewide application. The Governor's Task Force, which is an interagency steering committee made up of high level executives from various State agencies, reports to the Governor's Director of State Operations.

[1]In August 1997, legislation formally changed the name of the Governor's Task Force on Information Resource Management to the New York State Office for Technology.

Audit Scope, Objectives and Methodology

We examined the procedures used by seven State agencies and a public benefit corporation (agencies) to prevent the use of unlicensed software and protect against computer viruses during the period July 1, 1994 through February 20, 1997. The eight agencies, which together own about 19,000 microcomputers, include the Banking Department, the Department of Health, the Department of Motor Vehicles, the Department of Social Services, the Department of Transportation, the Empire State Development Corporation, the Insurance Department, and the Office of General Services. The objectives of our performance audit were to evaluate the adequacy of the procedures at the eight agencies, and to develop a list of "best practices" that could be used by State agencies. Additionally, these best practices could be of use to the Governor's Task Force in establishing statewide policies and procedures concerning the use of microcomputers at State agencies.

To accomplish our objectives, we interviewed officials and reviewed records at the eight agencies. We also tested the software installed on the microcomputers at five of the eight agencies. In addition, to identify commonly accepted practices for preventing the use of unlicensed software and protecting against computer viruses, we reviewed the relevant professional literature.

We did our audit according to generally accepted government auditing standards. Such standards require that we plan and do our audit to adequately assess the operations of the agencies which we include in our audit scope. Further, these standards require that we understand the agencies' systems of internal control and compliance with those laws, rules and regulations that are relevant to the operations which are included in our audit scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in the accounting and operating records and applying such other auditing procedures as we consider necessary in the circumstances. An audit also includes assessing the estimates, judgments and decisions made by management. We believe that our audit provides a reasonable basis for our findings, conclusions and recommendations.

We use a risk-based approach when selecting activities to be audited. This approach focuses our audit efforts on those operations that we have identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, finite audit resources are used to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations that may be relatively efficient or effective. As a result, our audit reports are prepared on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

Comments of the Governor's Task Force and Agencies' Officials

A draft copy of this report was provided to officials of the Governor's Task Force, as well as the eight agencies we audited, for their review and comments. The Governor's Task Force and the eight agencies generally agreed with our recommendations and indicated that actions were taken to implement them. In addition, in those cases where controls were in place, agency officials indicated that they would be reviewed to ensure that they were adequate and up to date. Their comments have been considered in preparing this report and are included in the report as appropriate, and attached in their entirely as Appendix B.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chairperson of the Governor's Task Force on Information Resource Management and the heads of the Banking Department, the Department of Health, the Department of Motor Vehicles, the Department of Social Services, the Department of Transportation, the Empire State Development Corporation, the Insurance Department, and the Office of General Services shall report to the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons therefor.

Unlicensed Software and Computer Viruses

We found that, in some instances, the eight agencies have developed, or are developing, and follow a number of appropriate procedures. Some of these procedures, which we summarize in Exhibit A, could be considered "best practices" and could be of use to the Governor's Task Force in its development of statewide guidelines. However, significant improvements can still be made in other procedures at each of the eight individual agencies. Because of control weaknesses at these agencies, the agencies' microcomputers are more likely to contain unlicensed software and computer viruses. In fact, when we tested 212 microcomputers at five of the agencies, we found that they contained a total of 246 unlicensed computer applications and three computer viruses.

Software Licensing

The Federal Copyright Act provides the rules that govern the right of a business to use and copy microcomputer software. Making unauthorized copies of a software product constitutes copyright infringement, for which the copier is subject to civil penalties and may be subject to criminal penalties. When someone purchases software for business use, every computer at that place of business must have its own set of original software. Purchasing a single set of original software to load onto more than one computer or to lend, copy or distribute without the prior written consent of the software manufacturer is contrary to the Federal Copyright Act. Running software protected by copyright on more than one machine simultaneously without a license from the software manufacturer is also contrary to the Federal Copyright Act. (When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software.) Organizations should not permit their employees to make copies of software that are not permitted by the software's license, and should obtain licenses commensurate with the number of copies in use.

To meet software licensing agreements, the Gartner Group, Inc., an internationally recognized technology consulting firm, suggests that organizations such as State agencies look for ways to monitor the actual use of computer applications. According to the Gartner Group, agencies must understand and comply with the vendor's licensing agreements and definition of concurrent use, and must ensure that the number of users is consistent with the licensing agreements. To meet these objectives, we believe agencies must maintain up-to-date hardware and software inventories, and periodically compare the inventories to purchase documents. The software inventory should include the type of license for each software application, the number of licenses or users, and the microcomputers on which the licensed software resides. Agencies should perform periodic surprise audits of the software

installed on microcomputers and should either delete any unlicensed software that is identified or purchase it legitimately.

In addition, according to guidelines developed by the Software Publishers Association to ensure compliance with software licensing agreements, organizations should (1) develop standard policies and procedures regarding the use of software; (2) develop a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements; (3) educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance; and (4) appropriately delegate responsibilities to ensure that the relevant policies and procedures are implemented as intended.

We examined the practices and procedures relating to the use of software at the eight State agencies included in our audit. We found that, in some instances, the agencies have developed, or are developing, and follow a number of appropriate policies and procedures. These policies and procedures, which are summarized in Exhibit A, could be considered "best practices" and could be of use to the Governor's Task Force in its consideration of statewide policies and procedures concerning the use of microcomputers at State agencies.

However, significant improvements can still be made in other policies and procedures at each of the eight individual agencies. For example, none of the agencies has a complete software inventory. Four of the agencies do maintain a list of their software applications, and these lists include the number of users or copies of the software. However, we found that the lists usually were not complete, mainly because some software was not included on the lists and the microcomputers containing the software were not indicated. We note that a proposed inventory practice at the Office of General Services may be particularly effective, as agency officials have made a group responsible for maintaining records indicating the software applications used by each program unit in the agency, including the specific microcomputers containing each application.

We also found that none of the agencies regularly performs surprise audits of the software installed on microcomputers. One agency verifies licensed software when rotating computers among staff and when upgrading software or hardware. However, these audits are not conducted on a surprise basis, which is important in detecting unlicensed software. Another agency requires its internal audit office to review software as part of its normal audits, but these audits look only for non-business software, not unlicensed software. A third agency identified unlicensed software during an audit, but does not perform such audits on a regular basis.

We further found that the eight agencies have developed or are developing a wide range of written policies and procedures regarding the use of unlicensed software. The procedures at some agencies are general with limited guidance, while the procedures at other agencies are specific and detailed. For example, some agencies specifically forbid the copying of agency software and the installation of unlicensed, unauthorized and personal software, including games. Two of the agencies require users to sign a statement that they will adhere to the policies and procedures.

Moreover, none of the agencies has a Code of Ethics concerning unlicensed software (during our audit, one agency did designate a group to work with management to create a clear statement of ethical behavior and appropriate use of computer resources), and none of the agencies has an education program to inform users about the importance of complying with software licensing agreements and the penalties for noncompliance. Some agencies have groups, individuals or supervisors who are responsible for communicating and enforcing policies and procedures relating to computer software, approving requests for and installing hardware and software, and performing and maintaining inventories. However, other agencies assign all these responsibilities to the individual units or users, and provide little or no guidance.

We believe the control weaknesses at the eight agencies can be attributed, in part, to a lack of statewide guidelines concerning the use of microcomputer software. We also believe that upper management at the agencies did not always emphasize the importance of procedures designed to prevent the use of unlicensed software, as we found few such directives from upper management at the eight agencies. We further note that the agencies have conducted few internal audits addressing microcomputer controls. Agencies' officials state they are limited in their staffing and funding resources, which sometimes makes it difficult to implement the required controls. Such limitations make it important to find other solutions, including the use of new technologies. We note that one agency is looking into automated software that can, from a central location, manage and audit the software inventory, including licenses, and prevent the installation of unauthorized software. Such a system could help to overcome the staffing and funding limitations.

As a result of these control weaknesses, officials at the eight agencies may not be aware of all the software applications residing on their microcomputers and whether they are properly licensed. To determine whether some of these software applications are in fact unlicensed, we judgmentally selected 212 microcomputers at five of the eight agencies (the Department of Health, the Department of Social Services, the Empire State Development Corporation, the Insurance Department, and the Office of General Services). We then used a specialized software package to review the contents of these 212 microcomputers. We reviewed the contents of between 33 and 49 microcomputers at each of the five agencies, which together have about 12,000 microcomputers.

We identified 246 unlicensed applications residing on the 212 microcomputers. These included 23 copies of a file compression utility, 109 games (which did not come bundled with the computer), 7 copies of a word processing package, 10 spreadsheet packages, and 97 other office, utility, communication, specialized and profession-related software packages. Agency officials told us they would either delete these applications or ensure that they were licensed. Officials at one agency told us that the game packages are available on the Internet. The officials believe employees may have downloaded the games on their home microcomputers and installed downloaded copies on agency microcomputers. Officials at another agency told us that they actually installed 150 copies of the unlicensed word processing package, but 143 copies were on machines that we did not test. The officials have placed a purchase order for all 150 installations.

We also identified another 86 applications (82 of which were games) on the 212 microcomputers that were not authorized by the agencies. We did not determine the license status for these 86 applications, but recommend that the agencies review these applications and either ensure they are properly licensed or remove them from the microcomputers.

Agencies that use unlicensed software are exposed to civil liabilities. According to The National Law Journal, "Every week, numerous software copyright infringement suits are filed. In 1991, the Software Publishers Association filed about two lawsuits a week around the country, seeking damages of $100,000 per violation plus attorney fees."
In addition, unlicensed copies of software may lack the quality controls built into the licensed versions, making the copies far more prone to computer viruses. Unlicensed software may also be an old version of the application with defects, incomplete files, or inadequate documentation; the data processed by such applications may not be reliable. Moreover, access to documentation, free technical support and upgrades are unavailable for unlicensed software.

We also note that, without an accurate software inventory reconciled to purchase documents, agencies might not take advantage of discounts or credits when upgrading the software. We found software on nine microcomputers that was not included on the agencies' inventory records. The software vendor offers a $230 per license discount for upgrading the package. The officials of one agency told us they were able to take advantage of $1,500 in software upgrade discounts after reviewing their software inventory information, based on our request.

Virus Detection and Eradication

Virus detection software helps prevent the introduction and spread of viruses from software brought from home, other offices, the Internet or any source.

To be most effective, virus detection software should run automatically upon start-up on at least a weekly basis. The software should also be able to be used to scan third-party software, data, and diskettes for viruses before use. The following practices are also effective in preventing computer viruses:

- Users should not be able to easily disable virus detection software.
- A log of virus infections should be maintained to make it easier to identify causes and prevent future occurrences.
- Users should be educated about computer viruses.
- An Internet policy should be developed informing users how viruses can be acquired through the Internet and how this can be prevented.

We examined the practices and procedures relating to the prevention of computer viruses at the eight State agencies included in our audit. We found that, in some instances, the agencies have developed and follow a number of appropriate policies and procedures. These policies and procedures, which are summarized in Exhibit A, could be considered "best practices" and could be of use to the Governor's Task Force in its consideration of statewide policies and procedures concerning the use of microcomputers at State agencies. For example, all eight agencies use virus detection software. At one agency, this software even alerts the user when it is time to update the software. At other agencies, the virus detection software is updated monthly and is distributed to users through a network.

However, significant improvements can still be made in other practices and procedures at each of the eight individual agencies, as some of the agencies do not ensure that the virus detection software is run on all machines on at least a weekly basis, and some of the agencies do not require that all software, data and diskettes from third parties be scanned for viruses before they are used. We also found that some users at most of the agencies can disable the virus detection software, and most of the agencies do not maintain a log recording the occurrences of viruses. We further found that none of the agencies formally educate employees about viruses, and five of the agencies do not have a policy concerning viruses and the Internet. Improvements are also needed in some of the Internet policies that have been developed, because they do not always completely describe how viruses can be acquired on the Internet.

We believe the control weaknesses at the eight agencies result from upper management not adequately emphasizing the importance of procedures designed to protect against computer viruses, as we found few such directives from upper management at the eight agencies. We also believe that the

weaknesses can be attributed in part to a lack of statewide guidelines concerning the use of microcomputers.

As a result of these control weaknesses, the microcomputers at the eight agencies are more likely to be infected with viruses. To determine whether these microcomputers were infected with viruses, we tested a judgmental sample of 99 microcomputers. The purpose of our test was to ascertain whether the virus detection software had been disabled and whether any of the computers had viruses. We found that the virus detection software had been disabled on 44 of 99 microcomputers, and three microcomputers had viruses. The virus detection software had been disabled on one of the three microcomputers with viruses.

The eight agencies recorded or estimated that they were infected by between 3 and 90 viruses a year. A total of about 120 staff hours were required to recover from a recent virus infection at one of the agencies. If the agencies do not improve their controls for preventing virus infections, they risk losing important data and incurring large recovery costs as a result of virus infections.

Recommendations

To the Governor's Task Force:

1. Consider the best practices summarized in Exhibit A as well as the other guidelines described in this report as the Task Force develops statewide microcomputer hardware and software policies and procedures.

   (Governor's Task Force officials endorse the recommendations in the report and identified areas where efforts have already begun. They advised that they have taken several actions to work with State agencies to develop policies and procedures. For example, the Governor's Task Force formed a Security Work Group (Group) composed of 16 individual from various State agencies. This Group developed a brochure entitled "Computer Security Awareness" that among other things, made agencies aware of the need for virus protection. In addition, the Group will consider the practices stated in the report for inclusion in a Best Practices and Preferred Standards document and will examine issues related to the items covered in recommendations 2 to 7.)

To the Eight State Agencies:

2. Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software.

3. Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance.
4. Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended.

5. Conduct internal audits addressing the controls over micro-computer software.

Recommendations (continued)

6. Delete or purchase any unlicensed software found on micro-computers.

7. Develop policies and procedures regarding computer viruses including, but not limited to:

   - all microcomputers be checked for viruses at least weekly,
   - all software, data and diskettes from third parties be checked for viruses before they are used,
   - users not be able to disable virus detection software,
   - a log of virus infections be maintained, and
   - users be educated about computer viruses, including viruses acquired through the Internet.

   (Officials from the eight agencies generally agreed with each of the above recommendations and indicated that they would implement new policies or procedures where necessary. However, officials at some of the agencies added that in many instances the recommended policy or procedure was already in place at their agency.)

   Auditors' Comment: We recognize that some of the agencies audited did have policies and procedures in place that cover some of the findings in this report, however, we intentionally made the recommendations broad to make them useful to not only the agencies that were audited, but also to the Governor's Task Force and agencies that were not included in the audit.

Best Practices

Policies and Procedures

- Provide users with written policies and procedures specifying software use is for business purposes only, copying of agency software is not permitted, and installing unauthorized and personal software (including games) is forbidden.
- Require users to sign off on policies and procedures.
- Remind users of policies and procedures with a memo annually.
- Require users to sign a request form each time they request a microcomputer or laptop. The request form should include all software and hardware being distributed and should state the policy that copying agency software, and installing and using unauthorized and unlicensed software and games is prohibited.
- Create a clear statement of ethical behavior and appropriate use of computer resources.

Software Inventories and Control

- Assign designated individuals the responsibility for approving software and hardware purchase requests and for installing and moving hardware and software.
- Assign designated individuals the responsibility for installing updates and maintaining the most current versions of all software.
- Assign designated individuals the responsibility for maintaining software inventories.
- Assign designated individuals the responsibilities for monitoring microcomputer software use and enforcing the related policies and procedures.
- Assign responsibility for performing software audits.
- Maintain a list of software from purchase documents, including the number of individual licenses or users.
- Designate a group to assemble and maintain a user profile of all program units in the agency listing all hardware, all applications and utilities, including the name of the application and machine it runs on, the initial installation date, a brief description of the applications and utilities, and who is responsible for operation and support.

- Use software that automatically prevents the installation of software identified by the agency as unauthorized.
- Require program managers and supervisors to be responsible for ensuring all computer usage adheres to agency standards and for maintaining proof of software ownership.
- Check for and remove unauthorized and unlicensed software when upgrading hardware and software and during reassignment of hardware.
- Ensure that software unrelated to work (including games) is not used and remove any such software that is found on agency microcomputers.
- Allow work-related software acquired by employees to be installed on agency microcomputers only if the software adheres to agency standards, the employee is licensed to use the software, and the use of the software is consistent with the license agreement.
- Ensure that downloaded software conforms to agency standards.

Virus Detection and Eradication

- Use virus detection and eradication software that runs automatically upon start-up.
- Designate a group to install virus detection software on all personal computers.
- Use virus detection software that alerts users that it is time to update the software.
- Use virus detection software on the agency network to automatically scan connected microcomputer hard drives and executable files.
- Require all files and software obtained from any outside source to be checked for viruses prior to transfer or installation.
- Develop an Internet policy requiring that downloaded freeware be checked for viruses.
- Instruct users on the procedures to follow when a virus is detected.
- Maintain a log of virus incidents.

Major Contributors to This Report

William Challice
David R. Hancox
Carmen Maldonado
Dominick Vanacore
Michael Pergament
Brian Reilly
Michael Heim
Richard Perreault
Robert Curtin
Debra Spaulding
James Thompson
Roslyn Watrobski
Dana Newhouse

STATE OF NEW YORK
EXECUTIVE CHAMBER
ALBANY 12224

Governor's Task Force
on Information Resource Management

JAMES G. NATOLI
CHAIRPERSON

CAMARON J. THOMAS
DIRECTOR
OFFICE OF THE TASK FORCE

October 1, 1997

Mr. David R. Hancox
Audit Director
Office of the State Comptroller
Alfred E. Smith Office Building
Albany, NY 12236

Dear Mr. Hancox:

The Office for Technology has received the Office of the State Comptroller's draft Audit Report (No. 96-S-51) entitled "Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies." To provide you with a coordinated response to your draft report, we have gathered the individual responses from each of the agencies covered by the audit. Below, we have provided you with our response to the recommendation posed to our agency as well as an overall response to each of the agency questions. In addition, we have attached the individual responses of each of the individual agencies listed in the audit as an addendum.

While we generally endorse the recommendations summarized in your report, we would also like to take this opportunity to point out the significant efforts that have been made by this Office in conjunction with State Agencies.

In April of 1996, the Governor's Task Force on Information Resource Management formed a "Security Work Group" composed of 16 individuals from State Agencies. This group developed a brochure entitled, "Computer Security Awareness" that was released in June 1996 to Agency Heads and Commissioners byJames Natoli, Director of State Operations. Among other things, this brochure made all agencies aware of the need for virus protection.

In January 1997, the Task Force issued Technology Policy 97-1 on information security. This policy addressed issues relating to viruses, downloading software, copyright and licensing, non-agency owned IT components, and virus protection. A copy has been attached for your review.

On June 5, 1997, Director of State Operations James Natoli sent out a letter requesting agencies designate a Technology Security Officer and identifying the need for New York State "to make computer and technology information systems security an even higher priority" than it had in the past; agency heads and commissioners were asked "to re-read this policy and fully understand its contents." The letter indicated that this policy touched upon many areas of information security including ".....information security, security management, ...and Employee (Agent) Responsibilities." At that time he noted that a companion document, the Standards and Best Practices for Information Security, was being developed to "bridge Technology Policy 97-1 with how an agency can adopt and implement its principles." To date, 60 Technology Security Officers have been designated to work with this Office to pursue compliance by all agencies.

On July 14, 1997, the Director of the Task Force forwarded a memorandum to IRM Directors requesting names of agency Technology Security Officers. A Security Round Table Discussion was then held on July 29, 1997 and was attended by Agency Technology Security Officers.

On August 20, 1997, IRM Directors were notified of a State Sponsored Security Awareness Day and the development of a Best Practices document through the efforts of the Security Work Group. This document will contain the State's preferred standards for security. The project will culminate in a training day for all Technology Security Officers prior to the implementation of the preferred standards.

In regards to the recommendations made specifically for the eight other agencies in your draft report, several have suggested that the Office for Technology address these issues under our existing Security Work Group rather than individually by each agency in order to insure a broader review of the issues as well as a more consistent approach.

The following responses are numbered to correspond with the recommendations in your draft audit:

1) The Security Work Group (referred to above) will consider the practices summarized in your report for inclusion in the Best Practices and Preferred Standards Document.

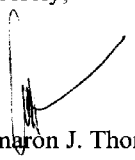
In addition, we will ensure that the Security Work Group will examine issues:

2) regarding software use, inventorying, and auditing;
3) emphasizing the importance of complying with the Federal Copyright Act and individual software licensing agreements; and include provisions regarding educating employees in this area;
4) identifying the need for agencies to actively follow-up to ensure policies and procedures relating to these areas are implemented as intended;
5) requiring agencies to develop methods of performing internal audits within their agencies where practicable;

6) develop an enhanced policy which outlines an appropriate method for dealing with unlicensed software; and
7) develop enhanced policies regarding computer viruses.

Please feel free to contact the Office for Technology at 518/473-5622 with any questions.

Sincerely,



Camaron J. Thomas

Att.
cc: State Agencies

STATE OF NEW YORK
BANKING DEPARTMENT
TWO RECTOR STREET
NEW YORK, NY 10006

September 29, 1997

David R. Hancox
Audit Director
State of New York Office of the Comptroller
A.E. Smith State Office Building – 13th Floor
Albany, NY 12236

Dear Mr. Hancox:

I am enclosing the Department's response to the draft audit report (96-S-51) pertaining to Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies pursuant to Section 170 of the Executive Law.

Very truly yours,

Gideon Weingarten
Director, Internal Audit

Encl.

CC: Elizabeth McCaul, Acting Superintendent
Ronald L. Minafri, Director Information Systems Management
Wael A. Hibri, Chief of Information Technology
Deirdre A. Taylor, Associate Budget Examiner, Division of Budget, Albany
John Cape, Budget Examining Unit Head, Division of Budget, Albany
Joseph J. Burns, Albany
[illegible], Albany

Response to Draft Audit Report 96-S-51
"Controls Relating to Licensed Software and Computer Viruses"

General Comment

Our response is limited to the general recommendations in the report (two through seven, since recommendation one is directed to the Governor's Task Force on Information Resource Management). The Banking Department was not selected for testing to determine unlicensed software applications and viruses on microcomputers. However, we are confident that our strong policy against such activity, known to all employees, acts as an effective deterrent to employees from putting unlicensed software on microcomputers thereby subjecting the computers to viruses. The policy makes it clear that it is unacceptable to install unlicensed and/or unpurchased software, and anyone caught doing so is subject to disciplinary action. Nonetheless, we concur with the conclusions stated by the audit report and offer the following.

Specific Comments

Recommendation: *Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software.*

Response: The Banking Department has started the expansion of the hardware inventory control system to include a software tracking sub-system. This work is expected to be completed by end of FY 1997-1998.

Recommendation: *Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance.*

Response: E-Mails regarding the compliance with the Federal Copyright will be sent to all Department users on a semi-annual basis as a reminder. In addition, the Banking Department's legal division will develop a Code of Ethics for use by the Department in the near future.

Recommendation: *Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended.*

Response: We conduct annual software and hardware audits. This will continue.

Recommendation: *Conduct Internal Audits addressing the controls over microcomputer software.*

Response: The ISM Department is currently undergoing an Internal Audit which is addressing controls over microcomputer software, among other risks.

Recommendation: *Delete or purchase any unlicensed software found on microcomputers.*

Response: This is the practice at the Banking Department.

Recommendation: *Develop policies and procedures regarding computer viruses including but not limited to:*

- *All microcomputers be checked for viruses at least weekly*
- *All software, data and diskettes from third parties be checked for viruses before they are used*
- *Users not be able to disable virus detection software*
- *A log of virus infections be maintained, and*
- *Users be educated about computer viruses, including viruses acquired through the Internet.*

Response: Currently installed anti-virus software constantly checks memory for viruses. Third party disks are checked automatically upon loading. The Department's Help Desk maintains a problem log of all virus related calls that they service.

3

10/01/97 10:20 TX/RX NO.0868 P.002

Empire Development

Mitchell W. Miller
Deputy Commissioner
Administration

September 23, 1997

Mr. David R. Hancox
Office of the State Comptroller
A. E. Smith State Office Building
Albany, NY 12236

Re: Response to draft audit report (96-S-51)

Dear Mr. Hancox:

Thank you for the opportunity to respond to the prepared draft report. It is much more balanced and objective than the original report we received. While many of the recommendations made have merit and are currently in place or being put in place, some of the conclusions reached are questionable or inaccurate. Senior management is aware of the issues that were identified and has emphasized that management of the hardware and software being utilized by staff is critical. However, it must also be acknowledged that the whole concept of personal computing is one of empowering employees to better be able to perform their work and thereby increase productivity, i.e. a decentralization of control but not management. Communication with users, teaching them the value in following the procedures, explaining that it is their data and files that we are attempting to protect, making them partners in the process of protecting the organization's assets will be far more effective in the long run than creating an environment of total control.

Databases of hardware and software, identification of what software is existent on which computers, periodic and random audits to ensure compliance with the internal policies are suggestions which must be implemented. MIS staff have their training and experience in computer related fields. The more we can educate the users to police themselves and to communicate with MIS, to establish a compact and partnership between the two parties, the greater will be the effectiveness and results. However, we believe judgement is required regarding the frequency of audits depending upon the size of the organization and the location of the equipment. We also plan on installing software which will give us the ability to monitor the use and type of software from a centralized approach and will take action to eliminate unauthorized use. We are currently revising our electronic communications policies right now and will incorporate some of your recommendations into our new policies.

Virus protection was present on the personal computers tested. The fact that only 3

New York State Department of Economic Development
One Commerce Plaza Albany New York 12245
Tel 518 474 2873 Fax 518 473 9731

viruses were actually found on 212 personal computers speaks highly for the procedures that are in place by New York State. Based upon your own criteria, one would assume that there is a probability that over twenty viruses could be found. As most trade magazines show, the virus protection software doesn't catch everything, even when current with the latest updates. There is vulnerability in this area and there is no way to reduce the risk to zero. The organizations audited have done an excellent job minimizing this risk.

Another suggestion, which was not made, would be to move to centralized, concurent licensed software to obviate the necessity of one license per personal computer. This would reduce the total number of licenses necessary for the organization as a whole. Historically, this has been the path we have followed in our organization. It is also simpler to manage the number of licenses needed by executing auditing software on the server to analyze and verify actual usage of the products.

The study of the nine state entities is a well-done and important effort. It helps facilitate communication between various state agencies and determine best practices. Thank you for your assistance in aiding us in to improve our practices and policies.

Sincerely,

Mitchell W. Miller

DRAFT

GEORGE E. PATAKI
GOVERNOR

STATE OF NEW YORK
EXECUTIVE DEPARTMENT
OFFICE OF GENERAL SERVICES
MAYOR ERASTUS CORNING 2ND TOWER
THE GOVERNOR NELSON A. ROCKEFELLER EMPIRE STATE PLAZA
ALBANY, NY 12242

JOSEPH J. SEYMOUR
COMMISSIONER

DRAFT LETTER TO MR. DAVID HANCOX FOR COMMISSIONER SEYMOUR'S SIGNATURE

September 29, 1997

Mr. David R. Hancox
Audit Director
Office of the State Comptroller
A. E. Smith State Office Building
Albany, New York 12236

Dear Mr. Hancox:

The Office of General Services (OGS) has reviewed the draft audit report (No. 96-S-51) regarding an audit addressing controls relative to licensed software and computer viruses. OGS has prepared the following in response to the draft.

Recommendations:

2. Enhance policies and procedures required that:

- Software use be monitored.
- Complete up-to-date software inventory records be maintained.

OGS Response: OGS concurs. A project is already in progress to achieve these goals. OGS has acquired Systems Management Server (SMS) from Microsoft to collect inventory on PC hardware and software. SMS has been deployed on 33 percent of the agency's workstations with full deployment by June 30, 1998.

- Software inventory records be periodically reconciled to purchase documents.
- Periodic surprise audits be conducted of installed software.

OGS Response: OGS concurs. The OGS Internal Audit Unit will undertake the responsibility.

3. Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance.

OGS Response: OGS concurs.

4. Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended.

OGS Response: OGS concurs.

5. Conduct internal audits addressing the controls over microcomputer software.

OGS Response: OGS concurs. The OGS Internal Audit Unit will undertake the responsibility.

6. Delete or purchase any unlicensed software found on microcomputers.

OGS Response: OGS concurs.

7. Develop policies and procedures regarding computer viruses including, but not limited to:

- all microcomputers be checked for viruses at least weekly,
- all software, data and diskettes from third parties be checked for viruses before they are used,
- users not be able to disable virus detection software,
- a log of virus infections be maintained, and

- users be educated about computer viruses, including viruses acquired through the Internet.

OGS Response: OGS concurs. Policies have been put in place to accomplish all of the recommendations above.

If there are matters in this response you would like to discuss, please have your staff contact Franklin Hecht at 474-4546 so that we may respond to your questions.

We appreciate your cooperation on this matter.

Sincerely,

/s/Joseph J. Seymour

New York State Insurance Department
September, 1997

The following is the New York State Insurance Department's Response to the Draft Audit Report issued by the OSC "Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies." The response predominantly addresses the recommendations set forth by the Comptroller. It should be noted however, that some of the commentary as it relates to the Insurance Department is not correct. The Insurance Department does maintain an inventory of software and certainly examines all opportunities to benefit from discounts.

The Insurance Department (Department) agrees that certain control structures could benefit from an updated review. Department management considers systems related controls very important. Below are comments concerning the Draft report's recommendations.

Recommendation:

"Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software."

Response:

The Insurance Department has a control process in place and always seeks to strengthen policies and procedures.

Recommendation:

"Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance."

Response:

The Department has a policy statement on the legitimate use of software and the prohibition of unauthorized use which all employees must sign. We will reissue this policy statement and in conjunction with overall internal control training emphasize system controls and appropriate use. The Department will explore other methods to ensure proper awareness and coverage.

Recommendation:

"Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended."

Response:

The Department has strong policy statements relating to unlicensed software. We will review our microcomputer program to ensure that policies and procedures are operating as intended.

Recommendation:

"Conduct internal audits addressing the controls over microcomputer software."

Response:

As resources permit, reviews will be conducted.

Recommendation:

Delete or purchase any unlicensed software found on microcomputers.

Response:

This has been the long-standing policy of the Insurance Department.

Recommendation:

Develop policies and procedures regarding computer viruses including, but not limited to:

- all microcomputers be checked for viruses at least weekly,
- all software, data and diskettes from third parties be checked for viruses before they are used,
- a log of virus infections be maintained, and
- users be educated about computer viruses, including viruses acquired through the Internet.

Response:

The Department currently uses anti-virus software. In the current fiscal year the Department has requested an upgrade to new anti-virus software for both the servers and the desktops. The new software will continuously monitor memory for viruses and scan diskettes and files upon loading. The Help Center currently maintains a log of all calls related to viruses.

STATE OF NEW YORK
DEPARTMENT OF MOTOR VEHICLES
EMPIRE STATE PLAZA
ALBANY NEW YORK 12228

RICHARD E. JACKSON, JR
COMMISSIONER

GREGORY J. KLINE
DEPUTY COMMISSIONER
FOR ADMINISTRATION

September 23, 1997

Mr. James G. Natoli
Chairperson
Governor's Task Force on
Information Resource Mgnt.
State Capitol
Albany, NY 12224

Atten: Bruce Oswald

Dear Mr. Oswald:

As requested, attached is this Department's response to the draft audit report, entitled "Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies" (96-S-51) to be included with your transmittal to the Office of State Comptroller.

Sincerely,

Gregory J. Kline
Deputy Commissioner

bj
Attachment

Department of Motor Vehicles
Reply to Draft OSC Audit Report
Licensed Software and Computer Viruses
Report 96-S-51

Recommendations to Governor's IRM Task Force:

1. *Consider the best practices summarized in Exhibit A as well as the other guidelines developed in this report as the Task Force develops statewide microcomputer policies and procedures.*

   We strongly agree with this recommendation. It is neither effective nor efficient for each agency to develop their own policies and procedures without some central guidance and uniformity.

Recommendations to the Eight State Agencies:

2. *Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software.*

   a. In the absence of Statewide policies, we are in the process of finalizing policies on microcomputer hardware and software use. We have used guidelines issued by the Governor's Task Force to develop draft policies on use of electronic mail and the Internet.

   b. The Department of Motor Vehicles will begin maintaining complete, up-to-date inventory records for software.

   c. We will periodically reconcile software inventory records to purchase orders, most likely in routine audits of our Data Processing Customer Service unit.

   d. In the future, we will conducting surprise audits of installed software on a sample basis. We will expand our review of installed software in periodic internal audits of various Department units.

3. *Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance.*

   We believe that this can be addressed in the new microcomputer policies and/or the next revision of the Department's Employee Handbook.

4. *Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended.*

   We agree that this is a goal that should be reached.

5. *Conduct internal audits addressing the controls over microcomputer software.*

   We will begin conducting internal audits addressing controls over microcomputers. We will continue to include a microcomputer audit procedure in each audit of various Department organizations.

6. *Delete or purchase any unlicensed software found on microcomputers.*

   Managers and supervisors will be instructed to delete or purchase unlicensed software when noted.

7. *Develop policies and procedures regarding computer viruses including, but not limited to:*
   a. *all microcomputers be checked for viruses at least weekly,*
   b. *all software, data and diskettes from third parties be checked for viruses before they are use,*
   c. *users not be able to disable virus detection software,*
   d. *a log of virus infections be maintained, and*
   e. *users be educated about computer viruses, including viruses acquired through the Internet.*

   Our proposed microcomputer and Internet policies will address dealing with viruses. They will advise users to always check software, data, diskettes from another source. While we can require users to check for viruses weekly, enforcing that requirements would be problematic.

   We are unaware of any virus detection software that a knowledgeable user would be unable to disable. Consequently, we do not find this recommendation one that can be implemented.

   Our Data Processing Customer Service unit will maintain a log of virus infections. We will continue to educate users about viruses through periodic means: electronic mail advisories, routine audits, etc.

STATE OF NEW YORK
DEPARTMENT OF TRANSPORTATION
ALBANY, N.Y. 12232

JOSEPH H. BOARDMAN
COMMISSIONER

GEORGE E. PATAKI
GOVERNOR

September 24, 1997

Mr. David R. Hancox, Audit Director
Division of Management Audit
Office of the State Comptroller
A. E. Smith Office Building
Albany, New York 12236

Dear Mr. Hancox:

I am writing in connection with your draft audit report 96-S-51, *Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies.* I am encouraged to learn that many of the practices and policies we have in place or have been considering are identified as best practices by your audit team. Specific comments on your audit recommendations follow.

Recommendation 2: "Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software."

Department Response: We agree with the recommendation. Our first policy statement on personal computer software was issued on November 15, 1996, a copy of which was provided to the audit team. Many elements of our policy were identified as "best practices" by the audit. The draft audit report is particularly timely, as we have had an effort underway to refresh and reissue our policy statement on personal computer software. We will carefully consider other suggestions presented in the audit report and will revise and reissue the policy statement by November 15, 1997.

The Department currently does not have the electronic infrastructure to maintain a useful software inventory centrally. However, our software policy provides clear direction to program managers on maintaining records of ownership. We are also gradually expanding our computer network and hope to be in the position in several years where virtually all personal computers are networked. This will give the Department the capability to maintain a software inventory electronically.

Recommendation 3: "Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance."

Department Response: We agree with and have already implemented the recommendation. The key elements are largely covered by our software policy issued on November 15, 1996. Technology Policy 97-1 issued by the Office for Technology (OFT) provides guidance to agencies relative to copyright and licensing of software and virus protection. If additional guidance or a Code of Ethics is necessary, we would suggest that OSC and OFT collaborate to expand the scope of Technology Policy 97-1 to provide this guidance for all agencies as an alternative to requiring individual agencies to independently develop this guidance.

Recommendation 4: "Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended."

Department Response: We agree with the recommendation. In the long term, the Department will complete the development of its microcomputer infrastructure. This infrastructure will allow for electronic software distribution, software inventory maintenance and monitoring compliance with Department policies. In the meantime, we will continue to underscore the importance of compliance by instructing supervisors, who have been charged with the ensuring compliance, to remove unlicensed software as they discover it.

Recommendation 5: "Conduct internal audits addressing the controls over microcomputer software."

Department Response: We agree with the recommendation that software and computer virus controls should be audited and therefore intend to prioritize these efforts among other program and functional areas as appropriate through Internal Audit's risk assessment process and management requests. Audits are conducted on both an announced and unannounced basis. In addition, Internal Audit has a formal role in providing internal control and process improvement recommendations to program managers for all proposed policy and procedural issuances. Future proposed policy and procedural statements from the Support Services Bureau will continue to be forwarded to Internal Audit for review and comment.

Recommendation 6: "Delete or purchase any unlicensed software found on microcomputers."

Department Response: We agree with the recommendation. The removal of unlicensed software is clearly required in the Department's personal computer software policy. Supervisors are given the responsibility for ensuring that their groups are in compliance with the Department's personal computer software policy. Automation support staff are available to remove unlicensed software, if needed.

Recommendation 7: "Develop policies and procedures regarding computer viruses including, but not limited to:

- all microcomputers be checked for viruses at least weekly,
- all software, data and diskettes from third parties be checked for viruses before they are used,
- users not be able to disable virus detection software,
- a log of virus infections be maintained, and
- users be educated about computer viruses, including viruses acquired through the Internet."

Department Response: We agree with the recommendation. Virus detection is addressed in a separate section of DOT's software policy issued November 15, 1996. In addition, the Department will issue a detailed technology procedure by December 15, 1997 providing specific guidance to employees on virus detection and eradication. The audit report recommends that users not be able to disable virus detection software. As a point of information, users need to disable virus detection software in order to perform software installations. Furthermore, we are not aware of any leading commercial software package that prevents users from disabling use of the package or modifying settings.

Thank you for the opportunity to comment on your draft audit report.

Sincerely,

Steven F. Lewis
Year 2000 Project Group

Department of Health Comments on the Office of the State Comptroller's Draft Audit Report 96-S-51 Entitled "Controls Relating to Licensed Software and Computer Viruses"

Recommendation 1 was directed to the Governor's Task Force; therefore, no response is provided.

Recommendation #2: Enhance policies and procedures requiring that software use be monitored, complete up-to-date software inventory records be maintained, software inventory records be periodically reconciled to purchase documents, and periodic surprise audits be conducted of installed software.

Response #2: Historically, the department has granted substantial control of information technology, and its implementation, to the program areas using that technology. This is especially true at the desktop level. Accordingly, development of agency-wide inventories and software audits represents a significant departure from past agency practice.

Nonetheless, the department recognizes the validity and importance of this recommendation. Software monitoring could be achieved in several ways; three possible approaches are:

- installing Local Area Networks (LANs) throughout the department and installing metering software on each LAN. This software would count the number of copies of a particular application that are active at any given time. This approach would be very expensive since many offices are not currently connected to LANs. The additional cost of implementing this approach would include hardware (LAN servers, interface cards, hubs, etc.), software (the LAN operating system and metering software), and personal service (LAN administration).

- installing a third party software package to perform license tracking. Such a package would query network servers across a wide-area network (WAN). Although the vendor of one such package indicates the excess traffic will be nominal, testing the product will be the only true measure of the added network traffic and impact on performance. A produce like this might require a purchase of a new server. In addition, the software cost of a representative product is approximately $40,000 for a 5,000-user license. Again, staff time would be expended to establish, maintain, support and review the additional logs.

- manually auditing each PC, matching it to hardware and software purchases and entering the data into a database. Since PCs can move and software be installed very easily, the inventory records would be out of date very quickly. This approach would be very resource-intensive and is probably the most costly approach. At present, the department is involved in a massive groupware implementation, made somewhat more complex by tile assimilation of a large number of former Department of Social Services employees. The department could not undertake a manual PC audit in the foreseeable future.

Department staff will explore the second option, WAN-based license tracking, for possible implementation.

Recommendation #3: Develop and communicate a Code of Ethics to emphasize the importance of complying with the Federal Copyright Act and individual software licensing agreements, and educate employees in the various types of licensing agreements, the need to comply with the agreements, and the consequences of noncompliance.

Response #3: The department provided a copy of Administrative Policy and Procedure Manual (APPM) item 425.0, entitled "Computer User Requirements/Security," to the OSC auditors. In that APPM it states that employees are responsible for: "Adhering to the copyright instructions of all computer software, and when not known, consulting with the ISHS security officer for assistance. (Note: Unless there is information to the contrary, the assumption must be made that copying of the software is unauthorized.)" Every employee receives a copy of this item and has access to all APPMs using a full text search capability. Although this portion of the APPM is not labeled as a "Code of Ethics", it would seem to perform the same function.

Recommendation #4: Actively follow up to ensure that the policies and procedures relating to unlicensed software are implemented as intended.

Response #4: If the department chooses to implement the type of tracking software described in response 2 above, a determination would have to made about how best to use the resultant data and ensure compliance with procedures.

Recommendation #5: Conduct internal audits addressing the controls over microcomputer software.

Recommendation #6: Delete or purchase any unlicensed software found on microcomputers.

Responses #5 and #6: The DOH will advise its program managers to take immediate steps to rectify this situation

Recommendation #7: Develop policies and procedures regarding computer viruses including, but not limited to:

- all microcomputers be checked for viruses at least weekly;
- all software, data and diskettes from third parties be checked for viruses before they are used;
- users not be able to disable virus detection software;
- a log of virus infections be maintained; and
- users be educated about computer viruses, including viruses acquired through the Internet.

Response #7:

- Checking all microcomputers periodically for viruses requires that antivirus software is installed on all desktop devices, and that it is run regularly. The department's desktop infrastructure includes devices running Windows 3.1, Windows 95, Windows NT, and Unix. It would be a complex task to implement antivirus software on all such devices. Department staff will develop a cost estimate for installing antivirus software on all Intel-based PCs. Once costs are determined, appropriate next steps will be taken.
- A policy will be developed regarding software and diskettes from foreign (i.e. outside the department) computers.
- The recommendation that users not be able to disable virus detection software is virtually impossible to implement; from a standalone PC, the user will always be able to disable the virus detection software. The department will, however, alert users that such software should not be disabled and will periodically monitor compliance.
- We suggest that it would be more useful, in the event of a virus having been detected, for the affected users to post a notification that a virus had been detected, the nature of the virus, the time of detection, and so forth. This is a generally ongoing protocol within the department,

- The department will develop and distribute informational material regarding computer viruses, including viruses acquired through the Internet.

In summary, the point at which virus detection is crucial is within the network; it is essential to ensure that viruses cannot infect LAN servers, nor be propagated across a LAN. Within the DOH, as funding is available, virus detection software will be installed on LAN servers. We will also be evaluating our Internet connectivity infrastructure to determine the best way to protect ourselves against Internet-borne viruses.

NEW YORK STATE
DEPARTMENT OF SOCIAL SERVICES
RIVERVIEW CENTER
40 NORTH PEARL STREET, ALBANY, NEW YORK 12243-0001

Brian J. Wing
Commissioner

David P. Avenius
Deputy Commissioner
Management Support and
Quality Improvement

September 29, 1997

Mr. Bruce Oswald
Office of Technology
State Capitol
Executive Chamber
Albany, New York 12224

Dear Mr. Oswald:

Pursuant to your discussion with David Dorpfeld of my office, we are forwarding the attached comments from our Systems Support and Information Services Division. It is our understanding that these comments will be included with those of other state agencies to form a single response to the State Comptroller's draft audit #96-S-51, entitled "Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies".

If you have further questions, please call Mr. Dorpfeld at 474-9748.

Sincerely,

James White
Director, Audit and
Quality Control

Attachment

cc: Henry Stone
Dave Dorpfeld

SSIS staff have reviewed the Office of the State Comptroller's report on "Controls Relating to Licensed Software and Computer Viruses". Before providing specific comments on the recommended best practices, we would like to offer the following general comments. First, many of the best practices mirror procedures that are and have been in place for many years in DSS. Second, with the move to a client-server architecture in modernizing our major production systems, the need for an enhanced level of security requires us to enforce many of the best practices features as standard business practices. Examples of this are provided in our specific responses. Finally, while no individual agency is mentioned by name in the report, given the number of best practices that we already have in place, we are sure that the Department was viewed favorably in the report.

Our specific comments on each best practice recommendation are provided below.

Statement: Provide users with written policies and procedures specifying software use is for business purposes only, copying of software is not permitted, etc.

Response: The Department has a long standing policy dealing with these issues. Since it was issued in 1986, it probably warrants revisiting to bring it up to date and insure that it is integrated into procedures which have been put in place subsequent to the development of the policy. The perfect forum for presenting such a written policy would be at our OA Network Administrators meetings (the next one which is scheduled in mid-October).

Statement: Require users to sign off on policies and procedures/Remind users of policies with a memo annually.

Response: This suggestion can be implemented via the "Inventory Control Sheet" which accompanies each PC upon delivery with the completed signature sheet being returned to the Inventory Control Unit. Annual reminders can be facilitated through on-line system broadcasts. I will communicate this suggestion to Inventory Control personnel.

Statement: Require users to sign a request form each time they request a microcomputer or laptop.

Response: The Department has such a process in place. All DSS microcomputer equipment acquisitions are based on a formal, documented request/approval process. The DSS Computer Store, which lends computer equipment to Department staff, requires a signature document, which specifies the suggested language, prior to extending the loan.

Statement: Create a clear statement of ethical behavior and appropriate use of computer resources.

Response: This will be made part of the written policy document identified in item 1 above.

Statement: Assign designated individuals the responsibility for approving software and hardware purchase requests and for installing and moving hardware and software.

Response: The designated office for such activity within DSS is the Computer Store organization. Software installation activities as identified in this statement, are facilitated via DSS staging of "image" disks which are then sent to the appropriate manufacturers. Organization Network Administrators have this responsibility subsequent to the initial installation.

Statement: Assign designated individuals the responsibility for installing updates and maintaining the most current versions of all software.

Response: This function has been largely relegated to the Department's Network Administrators. The Administrators possess the knowledge and system resources required to affect updates as they become available/warranted.

Statement: Assign designated individuals the responsibilities for monitoring microcomputer software use and enforcing the related policies and procedures.

Response: This function has been largely relegated to the Department's Network Administrators.

Statement: Assign responsibility for performing software audits.

Response: This function is presently a function of the Department's Office of Internal Audit.

Statement: Maintain a list of software from purchase documents, including the number of individual licenses or users.

Response: The Computer Store organization presently reconciles all requests for software products to purchase, vendor bill-of-lading and delivery documents. In the case of license purchases, all quantities are reconciled to original requests and deliveries.

Statement: Assemble and maintain a user profile of all program units listing all hardware, applications and utilities.

Response: While the Department maintains a detailed inventory system of device by user, the inventory information does not, at this time, extend to what software is loaded on what machine. This information is however available through the Computer Store Request/Approval Unit at the organizational unit rather than the individual machine level.

Statement: Use software that automatically prevents the installation of software identified by the agency as unauthorized.

Response: We are unaware of the existence of such a software package. The CONNECTIONS project has taken a different approach which the Department will probably use in other major PC initiatives such as CSMS and WMS Redesign. PCs, using the security capabilities of Windows NT, are set up so that the ability to install software is generally restricted to individuals who are assigned Administrator rights.

Statement: Require program managers and supervisors to be responsible for ensuring all computer usage adheres to agency standards and for maintaining proof software ownership.

Response: Department policy and procedures currently meet this recommendation. These policies need to be reinforced and will be made a discussion topic in Network Administrator meetings.

Statement: Check for and remove unauthorized and unlicensed software when upgrading hardware and software and during reassignment of hardware.

Response: This should be made a responsibility of the Network Administrator for each office/project area. In order to pass along this responsibility, the Department needs to give consideration to formalizing the role of the administrator.

Statement: Allow work related software acquired by employees to be installed on agency microcomputers only if the software adheres to agency standards.

Response: Generally, the Department requires prior approval for installation of "non-standard" employee acquired software. Continued use of employee acquired products must be legitimized through purchase of licenses as appropriate.

Statement: Ensure that downloaded software conforms to agency standards.

Response: All software installed on Department PCs must meet agency standards, regardless of source. At this time, Internet access throughout the Department is severely restricted making this less than a significant concern. In addition, the Department is piloting Firewall technology which could be used to limit the ability to access and download software.

Statement: Use detection and eradication software that runs automatically upon start-up.

Response: The Department presently has a site-license with McAfee Software for distribution and use of that firms complete set of virus detection programs. Depending on the hardware/operating system platform of the individual workstations, virus scanning may/may not be set to execute automatically. The CONNECTIONS project PCs all have IBM's anti-virus software installed which automatically initiates a daily scan. This technological approach will be used in future PC initiatives.

Statement: Designate a group to install virus detection software on all personal computers.

Response: The Computer Store organization is responsible for maintaining the site license with McAfee Software and for acquiring the latest update products from that firm. Network Administrators are responsible for installing the appropriate products on workstations/servers within their respective organizations.

Statement: Use virus detection software that alerts users that it is time to update the software.

Response: McAfee virus protection products provides this automatic alert feature.

Statement: Use virus detection software on the agency network to automatically scan connected microcomputer hard drives and executable files.
Response: Automatic virus scanning is the recommended approach on the Department's servers. Because we depend on the organizational Network Administrators it is not currently consistently implemented. We will reinforce the process and responsibility with the Network Administrators.

Statement: Require all files and software obtained from any outside source to be checked for viruses prior to transfer or installation.
Response: This is the recommended policy. Awareness of risks associated with not performing pre-scans needs to be addressed at Network Administrator meetings.

Statement: Develop an Internet policy requiring that downloaded freeware be checked for viruses.
Response: See the response above. The Department's policy recommends scanning regardless of the source of the software.

Statement: Instruct users on the procedures to follow when a virus is detected.
Response: The Department has such a procedure in place through its Network Administrators and through the support lent by the Computer Store.

Statement: Maintain a log of virus incidents.
Response: A log of reported calls is maintained by the Computer Store HelpLine organization in Support Magic helpdesk software.

STATE OF NEW YORK
DEPARTMENT OF MOTOR VEHICLES
EMPIRE STATE PLAZA
ALBANY NEW YORK 12228

RICHARD E. JACKSON, JR.
COMMISSIONER

GREGORY J. KLINE
DEPUTY COMMISSIONER
FOR ADMINISTRATION

September 23, 1997

Mr. David R. Hancox
Audit Director
Bureau of Management Audit
A. E. Smith State Office Building
Albany, New York 12236

Dear Mr. Hancox:

In response to your September 2, 1997 transmittal of the draft audit report, entitled *Controls Relating to Licensed Software and Computer Viruses at Selected State Agencies.*(96-S-51), the Department of Motor Vehicles has prepared a reply addressing the recommendations contained in that report. This reply has been forwarded to the Division of the Budget for clearance, as required by Budget Policy and Reporting Manual Item B-410.

In addition, the Department of Motor Vehicles' response to this draft audit report will be furnished to Mr. James G. Natoli, of the NYS Office for Technology. Mr. Natoli has indicated that all replies for the affected agencies would be transmitted to your attention, under his signature.

Please feel free to contact me if any further information is needed.

Sincerely,

Gregory J. Kline
Deputy Commissioner