The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

NO. 2004-0089-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY-RELATED CONTROLS FOR VIRUS PROTECTION AT THE MASSACHUSETTS STATE LOTTERY COMMISSION

October 9, 2003 through August 24, 2004

OFFICIAL AUDIT REPORT

JULY 12, 2005

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts State Lottery Commission (MSLC) is authorized by Chapter 10, Sections 22 through 35 of the Massachusetts General Laws to raise revenues for Massachusetts cities and towns and state and federal tax revenues by eliminating or minimizing illegal gambling and bookmaking operations and conducting and operating various legal lottery games. The Massachusetts State Lottery Commission is located in Braintree, Massachusetts and, in addition, they maintain six satellite offices.

The Commission’s business operations are supported by an IT configuration of a local area network (LAN) consisting of three file servers and three hundred workstations. The Commission maintains a blocking firewall to the Commonwealth’s Information Technology Division (ITD). The firewall was installed to provide increased access security and privacy essential to the operation and mission of the Commission. The Commission has connections to MAGNet, the Commonwealth of Massachusetts’ wide area network (WAN), and uses anti-virus software for scanning of the LAN and all individual workstations. The Commission has seven information technology positions that are responsible for the operations and security of IT infrastructure.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

Our audit, which was conducted from August 10, 2004 through October 25, 2004, consisted of an examination of virus protection activities at the Massachusetts State Lottery Commission for the period covering October 9, 2003 through August 24, 2004. Our examination focused on a review of controls related to policies, procedures and use of software tools to prevent and detect viruses and unauthorized intrusions, assess the level of risk of viruses, report on the occurrence of a potential virus, and to implement corrective measures. The audit was performed in conjunction with similar audits conducted at thirty-two other state agencies for the period covering October 2003 through January 2005 (see Appendix 1).

Audit Objectives

The primary objective of our audit was to determine whether the Commission’s IT resources were adequately protected against virus attacks and malicious intrusions through appropriate preventive, detective, and corrective measures. Specifically, we sought to determine whether adequate policies and procedures were in place to inform and guide personnel in addressing virus protection and to determine whether appropriate software tools, such as anti-virus software, were used to prevent and detect computer viruses. In addition, we sought to determine whether appropriate risk management procedures and tools were in place to limit malicious intrusions and virus entry points and to address vulnerabilities that viruses could exploit. We also sought to determine whether appropriate policies and procedures were in place to respond to detected viruses. Lastly, we determined the extent to which virus protection-related efforts were documented and monitored.

Audit Methodology

Before initiating audit field work, we researched generally accepted management and technical control practices that addressed virus protection. We conducted preliminary research on various anti-virus software programs and their capabilities. We also researched the use of firewalls, intrusion detection systems, anti-adware and anti-spyware programs, patch management, alert notifications, and documentation of incident response and remediation efforts. Research was also performed on IT-related virus activities, including the history, creation, detection, and eradication of computer viruses. Our pre-audit work included identifying standard procedures undertaken by the Commonwealth’s Information Technology Division (ITD) to address virus protection and to support agencies in detecting and eliminating viruses. We developed survey questions and audit procedures based upon recommended control practices, including the use of software controls to identify and eliminate computer viruses. Our survey questionnaire incorporated questions that focused on management and technical control practices used to address virus protection. The survey was developed to serve as a high-level checklist for agencies in reviewing their status with respect to generally accepted virus protection policies and procedures. Our pre-audit work included gaining and recording an initial understanding of the Commission's mission and business objectives through Internet-based research.

Our on-site audit work included verifying our initial understanding of the Commission's mission and business objectives and identifying the entity's IT environment and how IT resources were configured. To determine whether appropriate policies and procedures were in place to provide direction and guidance on addressing virus protection, we determined whether the Commission had identified the level of virus infection risk and established control mechanisms to mitigate the risk. We requested policies and procedures related to virus protection and other documentation regarding the use of anti-virus software. We reviewed and evaluated the Commission's stated policies and procedures regarding virus protection. We identified whether the Commission had access to MAGNet and were MassMail users, and the extent to which anti-virus programs had been deployed and kept up to date.

We interviewed the information technology personnel responsible for managing the IT environment to identify specific controls directed toward virus protection. We assessed the level of understanding of virus risks, use of anti-virus programs, and risk management and incident response procedures. With respect to protective measures, we determined whether the Commission's IT environment was subject to firewall protection, intrusion detection, and appropriate update and patch management procedures. Specifically, we ascertained whether the installed anti-virus software had been adequately maintained with the latest software and definition updates.

We reviewed the Commission's experience regarding virus attacks and the steps taken to protect their IT environment. We determined whether the Commission had incident handling procedures to investigate, isolate, and eliminate viruses if detected on IT equipment. In addition to enquiring how the Commission may have been effected by viruses, we documented the use of software to detect, eradicate, and prevent viruses. We determined whether control practices were in place to support safe recoveries under business continuity procedures should a virus render systems inoperable and recovery procedures needed to be initiated.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. The audit criteria used for our examinations were based on applicable control objectives and generally accepted IT control practices. Included in the report's Appendix is a list of generally accepted control practices for virus protection (see Appendix 2). In addition to generally accepted control practices, audit criteria for management control practices were drawn from Control Objectives for Information and Related Technology (CobiT). CobiT is a generally applicable and accepted standard for information technology security and control.

Virus Background And History

A computer virus is man-made software used to infiltrate and attack a computer's operating system, applications, or data files. In most instances, the attack happens without the knowledge of the computer's owner, with the first indication that an attack has occurred when the computer either does not work or starts to perform incorrectly.

The Massachusetts State Lottery Commission relies heavily on information technology, including access to MAGNet, to help carry out its mission and business objectives. We note that over the last few years MAGNet has experienced infection from computer viruses from time to time. According to ITD there have been fifteen successful virus attacks in the fifteen-month period from October 2003 to December 2004 (see Appendix 3). To maintain a record of the viruses, ITD in 2003 created a software program called Security Alert System (SAS) which allows ITD to track and rank the virus threats with a threat level of low, medium, high, and critical. According to ITD's threat table, there were 42 tracked virus incidents between October 9, 2003 and January 5, 2005 (see Appendix 4).

In order to protect the Commonwealth, ITD requires that agencies use anti-virus software; provides a downloadable copy of anti-virus software for agency use; maintains the SAS tracking program, a Help Desk, and firewalls; sends out alerts to IT personnel at state agencies; and monitors MAGNet so that agencies with virus infections are disconnected if necessary until the virus has been removed. ITD has also created policies that agencies are required to follow if they are to use ITD resources (see Appendix 5).

To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic anti-virus program needs to be established. There are two major ways to prevent and detect viruses and worms that infect computers and network systems. The first is by having sound policies and procedures in place, and the second is by technical means, including anti-virus software. Both administrative controls and technical tools are required to effectively provide virus protection.

AUDIT CONCLUSION

We determined that sufficient controls were in place at the Massachusetts State Lottery Commission to provide reasonable assurance that information technology resources would be adequately protected against known virus attacks through appropriate preventive, detective, and corrective measures. We determined that appropriate software tools were in place and in effect, such as anti-virus software, to prevent and detect computer viruses and questionable or malicious code.

Although we found that the Commission had appropriate procedures and control practices for virus protection, documented policies and procedures needed to be enhanced. We found that further documented guidance should be available regarding the impact of virus attacks and infection, and with respect to risk assessment and business continuity planning. Although the Commission's staff demonstrated sufficient knowledge in the steps to be taken to address virus infection, documented policies and procedures needed to include incident response procedures.

We determined that the Commission should document the assessment of virus-related risks and the impact of virus attacks and infection on IT operations and business continuity planning. While virus protection efforts appear to be monitored, documented status reports should be prepared for management review.

Due to the evolution of virus programs and the nature of virus attacks, the risk of virus infection can not be absolutely eliminated even though entities may have generally-accepted virus protection and security controls in place.

AUDIT RESULTS

We found that administrative controls and technical tools were in place to address virus protection. The Commission had certain policies and procedures in place regarding virus protection and all IT equipment, such as file servers and microcomputer workstations, had up-to-date anti-virus software installed. Although we found that the Commission had assessed the requirements for having anti-virus software installed on their IT equipment, documentation of the risk assessment was unavailable at the time of our review. According to the Commonwealth's Information Technology Division, the Commission has been infected on one occasion by viruses over the period from October 2003 to December 2004 (see Appendix 3).

While the Commission, as a client of the Commonwealth's wide area network, MAGNet, relies on the Information Technology Division's (ITD) firewall and intrusion detection services, to protect its IT resources, the Commission also operates behind its own firewall for additional security of IT data and applications systems. We found that ITD's firewall management addressed email filtering and blocking capabilities to ensure that all multi-part MIME messages will be blocked at the gateway, and that emails containing files with extensions, which are affiliated with a virus, are discarded. The Commission also relies on ITD to inform them of any virus and security alerts.

We found that digital security controls were in place to help limit the risk of unauthorized access or malicious intrusion. We found that stated controls regarding logical access security were appropriate and that generally accepted control practices were included in the Commission's documented policies and procedures. Furthermore, based upon our review, it appears that controls were in place to ensure that users cannot disable anti-virus software.

The Massachusetts State Lottery Commission's procedures require all disks, CD's or unknown files must be scanned with anti-virus software prior to installing or opening. We determined that the MSLC maintained their anti-virus and firewall programs with the most recent vendor updates in a timely manner. According to the Commission, vendor-provided updates, designated to be "critical security updates", were deployed in a timely manner after testing on a stand-alone computer.

We found that the Massachusetts State Lottery Commission needed to document their annual or periodic risk assessments that specifically identified and reevaluated virus vulnerabilities. The risk assessment should identify all existing virus access points, determine whether there have been changes to the IT configuration requiring updates to installed IT resources, and determine whether currently-installed anti-virus tools and procedures adequately meet virus protection objectives. While users may be familiar with the risks posed by viruses, user training specifically focused on virus protection and incident handling would be beneficial. We found that formal training had not been recently given to ensure that all users of computer equipment would be adequately educated regarding the risks of computer viruses, indications of infected machines, and notification and incident response procedures.

While the Commission relies on ITD to formally reevaluate virus protection, notification, and remediation measures following each virus attack, the Commission’s policy should require that they determine after a virus incident whether any changes to their virus protection efforts are needed.

Recovery procedures should require that all backup copies of data files and application and system programs, utilities and tools be scanned by anti-virus software as they are reinstalled. Policies should include that if performing a full restoration of the system to recover from a virus attack, one should ensure that current anti-virus software is installed prior to installing data files and application software and other utilities to enable appropriate scanning.

Recommendations:

We recommend that the Massachusetts State Lottery Commission enhance their IT policies and procedures regarding documentation of the assessment of the risk of virus attacks and infection, and the measures in place to mitigate that risk. We recommend that the Commission’s policies and procedures include a requirement that the adequacy of tools in place to help monitor and maintain network security be assessed upon major changes to technology or connections to external networks, or at least on an annual basis. To further strengthen documented policies, we suggest that access to the Internet from the Commission’s LAN-based environment be only through an approved Internet gateway, such as those going through firewalls or by VPN. Access to the Internet via modems or wireless should be prohibited. We recommended the Commission’s procedures also provide guidance to users on deleting non-recognizable emails and unknown or questionable attachments as well as prohibiting the downloading of executable (.exe) files. We recommend that documented policies be created to strictly prohibit the creation of computer viruses through the intentional writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any IT resources.

We recommend that the Commission benchmark their IT-related policies against those of ITD and assign responsibility for evaluating, updating, and monitoring compliance to ensure that the policies are in sync with each other For example, a review of policies would help ensure compliance with the requirement that instant messaging not be allowed within MAGNet.

With respect to virus protection on the part of users, we recommend that an appropriate level of formal training be provided to ensure that users have an adequate understanding of the Commission's virus protection policy and procedures, risks of computer viruses, indications of infected machines, and notification and incident response procedures. Training should include user responsibilities to install "critical" updates for which notification of the availability of the updates has been distributed or "pushed" to their microcomputer workstations.

We recommend that incident response policies and procedures be documented. Such policies and procedures should emphasize preventing security breaches through containment and eradication of the infection or problem. The procedures would include notification to ITD's Help Desk of a possible virus infection, guidelines for disconnecting IT resources from the internal network, and identifying and removal of suspected viruses. The guidelines should require that if a new threat has been reported, but a solution has yet to be made available, the Commission should continue to keep the computer disconnected from the network. From an administrative perspective, we recommend that virus protection policies and procedures be dated indicating version or tracking number and that employees be required to acknowledge receipt and understanding by signature of all IT user policies, which would include among other responsibilities, virus protection.

We recommend that the Commission consider the installation of anti-spyware and anti-adware software to run in addition to anti-virus software.

Auditee Response:

> *I have reviewed with Joseph Sullivan, the draft copy of your report on virus protection at the Massachusetts State Lottery Commission, #2004-0089-4T. As I see it, your recommendation is to increase our documentation and training efforts. I agree with that recommendation and, in fact, we have already begun the process.*

Auditor's Reply:

We agree with the Commission's efforts to further document their virus protection policies and procedures as well as provide training to their staff.

APPENDIX 1
Agencies Visited

Name

Architectural Access Board
Bureau of State Office Buildings
Commission Against Discrimination
Commission for the Deaf and Hard of Hearing
Department of Fish and Game
Department of Revenue
Department of Social Services
Developmental Disabilities Administration
Disabled Persons Protection Commission
Division of Career Services and Unemployment
George Fingold Library
Group Insurance Commission
Human Resources Division
Information Technology Division
Legislative Information Services
Massachusetts Highway Department
Massachusetts Hospital School
Massachusetts Office of Travel and Tourism
Massachusetts Office on Disability
Massachusetts Rehabilitation Commission
Massachusetts State Lottery Commission
Massachusetts Turnpike Authority
Merit Rating Board
Municipal Police Training Committee
Newton Housing Authority
Office of Child Care Services
Office of Inspector General
Office of Professional Licensure
Registry of Motor Vehicles
State Ethics Commission
Teachers’ Retirement Board
University of Massachusetts Boston
Victim and Witness Assistance Board

APPENDIX 2

Generally Accepted Management and Technical Control Practices for Virus Protection

Control	Type of Control	Applies to
Administrative Controls **Management Control Practices**		
Organizational policies should address virus protection. The virus protection policies should be documented and formally reviewed and approved and should include the following requirements: • To effectively reduce the risk of computer viruses and worms infiltrating an organization, a comprehensive and dynamic antivirus program needs to be established. There are two major ways to prevent and detect viruses and worms that infect computers and network systems. The first is by having sound policies and procedures in place, and the second is by technical means, including antivirus software. Neither is effective without the other. • All IT equipment, such as microcomputer workstations, laptops, and servers, must have up-to-date anti virus software installed. • All IT-related equipment upon which a virus could execute or propagate should be subject to anti-virus software. Virus scanning software should be installed at the workstation, LAN, WAN and Mail Server levels. • For all possible Internet gateways, access should be obtained through a firewall. IT equipment that connects to the Internet must be behind a firewall. • Prohibit access to the Internet or external networks through modems or by wireless. • Access to the Internet should only be through approved Internet gateways. • All updates should be reviewed or tested prior to installation. • Appropriate incident response procedures should be in place to guide entity personnel in identifying, quarantining and eradicating IT viruses.	Policy Preventive Detective Corrective	All IT environments

Control	Type of Control	Applies to
Organizations should assess the requirements for having anti-virus software installed in IT equipment in addition to workstations, notebooks, servers and mainframes. • Organizations should assess the need for software tools to scan, enhance access security, and push updates or patches to connected machines. • Organizations should assess whether the installation of an IPS or IDS is warranted to provide enhanced security. Organizations should assess whether the installation of anti-adware and anti-spyware software is warranted to provide enhanced security.	Policy Preventive Detective Corrective	All IT environments
The acquisition of additional software tools should be based upon risk analysis, cost, and resource capabilities to support and use the software.	Policy Procedure Preventive Detective	All IT environments
Removable media, software or files downloaded from the Internet, or unknown files, should be scanned with anti-virus software prior to installing or opening.	Policy Procedure Preventive Detective	All IT environments
All users of computer equipment should be trained regarding the risks of computer viruses, indications of infected machines, and notification and incident response procedures.	Policy Procedure Preventive	All staff
All security-related programs, such as firewall, intrusion prevention, intrusion detection, anti-virus and anti-spyware programs, should be maintained with the most recent vendor updates in a timely manner.	Policy Procedure Preventive	All security programs
Vendor-provided updates, designated or determined to be “critical updates” should be deployed in a timely manner after testing by the IT department or the security administrator.	Procedure Preventive	All Windows OS
Entities having anti-virus software installed on their workstations, notebooks, and servers where IT resources are configured in LANs or WANs should ensure that centralized monitoring and administration of anti-virus software is in effect.	Procedure Preventive Detective	All centralized control monitors
An objective of centralized monitoring and administration of anti-virus software For LAN and WAN environments is to ensure that all IT resources upon which anti-virus software is installed have the most recent versions of the anti-virus software. • Organizations should use software tools to the extent possible to determine whether IT resources have the most recent versions of anti-virus software installed when the resources log on. Organizations should consider implementing centralized capabilities to push software or updates.	Policy Preventive Detective	All centralized control monitors

Control	Type of Control	Applies to
Security and LAN administrators should determine in a timely manner as to whether notified alerts apply to their entity's IT environment.	Policy Procedure Preventive Detective	If no LAN or administering console, users must update
If applicable, Security and LAN administrators should determine whether established incident response steps should be followed, whether users should be notified and provided with instruction, and whether assistance should be requested.	Policy Procedure Preventive Detective	Security and LAN administrators
Management should ensure that backup copies of security-related software, such as firewall, intrusion prevention, intrusion detection, anti-virus and anti-spyware programs, are included with the backup copies of data files and application and system programs needed for the restoration of IT operations at an alternative processing site.	Policy Procedure Preventive	All recording media
All backup copies of data files and application and system programs, utilities and tools should be scanned by anti-virus software before use. • When performing a full restoration of the system to recover from a virus attack, one should ensure that current anti-virus software is installed prior to installing data files and application software to enable appropriate scanning.	Policy Procedure Preventive Detective	All recording media
Entities should perform periodic risk assessments to identify and re-evaluate gateway vulnerabilities. • The risk assessment should identify any existing virus and intrusion access points, determine whether there have been changes to the enterprise configuration requiring updates to installed IT resources or security-related software, and determine whether currently-installed anti-virus tools and procedures adequately meet virus protection objectives.	Policy Procedure Preventive	All IT environments
All reasonable steps should be taken to eliminate the sources of viruses. Recipients of emails for which the sender is unknown should consider deleting the emails without opening them.	Policy Procedure Preventive	All users
Only authorized software should be installed on IT systems. • Management should inform the IT user community as to what has been designated as the enterprise's approved or "authorized software." • Installation of software obtained from external, non-agency sources should not be installed onto agency systems unless reviewed and approved by management. All software should be reviewed and tested on an isolated machine or environment before being installed on the entity's system.	Policy Procedure Preventive Detective Corrective	All users
Incident response policies and procedures should emphasize preventing security breaches through containment and eradication of the infection or problem. • Incident response procedures should include: planning and notification, identification and assessment of the problem, containment and quarantining of the problem, eradication of the problem, recovering from the incident, and the follow-up analysis. Incident response should never include retaliation.	Policy Procedure Preventive Detective Corrective	All IT administrators

Control	Type of Control	Applies to
Entities should have access to alert information to ensure that they are aware of potential or new virus-driven risks and new critical security risks, either directly from a alert provider or by relying on a trusted source external to the entities. (Alerts may be obtained from a Commonwealth source, such as ITD)	Policy Procedure Preventive	All agencies
Infected computers with reported viruses without solutions require keeping the computer off the network until a solution is found.	Policy Procedure Preventive	All staff
Following each virus attack, agencies should formally re-evaluate virus protection, notification, and remediation measures and procedures to promote sufficient understanding of the event and how it was resolved, and to determine whether changes to virus protection should be incorporated into contingency planning, notification, and remediation measures.	Policy Procedure Corrective	All staff
End users should be administratively restricted from disabling or uninstalling anti-virus or security-related software.	Policy Procedure Preventive	All staff
Policies should strictly prohibit the creation, copying, or propagating of computer viruses.	Policy Procedure Preventive	All users
Each user is responsible for the IT resources assigned to, or used by, them (computer and peripherals). When an infection due to malicious code is suspected, the user should immediately stop computing and follow the emergency procedure provided by management and/or the security officer. In addition he/she should inform the appropriate parties (security department, help desk, etc.) about the problem in order to mitigate consequences and probability of malicious code propagation within the organization. If the user is not able to follow the procedure, he/she should immediately power off the computer and call the appropriate party (security department, help desk, etc.) for assistance.	Policy Procedure Preventive	All users
Management should assign responsibility for evaluating, updating, and monitoring compliance with IT policies.	Policy Procedure Preventive	Administrators
Employees are required to acknowledge receipt and understanding of IT policies relating to their responsibilities for the integrity, security, use and availability of IT resources.	Policy Procedure Preventive	All users
Policies should be reviewed and approved by IT and entity management and be dated with appropriate version or tracking numbers included.	Policy Procedure Preventive	IT and entity management
Technical Controls		
All IT equipment, such as PCs, laptops, and servers must have up-to-date anti-virus software installed.	Policy Procedure Preventive	IT Administrators
There should be a firewall for all possible Internet gateways.	Policy Procedure Preventive	IT Administrators

Control	Type of Control	Applies to
Anti-adware and anti-spyware software should be used in addition to anti-virus software for protection of unauthorized intrusion.	Policy Procedure Preventive	All IT environments
Ensure that insecure protocols are blocked by the firewall from external segments and the Internet.	Policy Procedure Preventive	IT Administrators
The use of Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) should be in concert with firewalls.	Policy Procedure Preventive	IT Administrators
No portable drive, including floppy disks, CDs, DVDs, or USBs, or any other portable electronic media shall be connected to a workstation or server on the network that is not running an up-to-date version of anti-virus protection.	Policy Procedure Preventive	All workstations, LAN environment
All connections to external or third-party entities should be monitored and should pass through a firewall.	Policy Procedure Preventive	All MAGNet agencies
To access the Internet from LAN or WAN environments, organizations should only use approved Internet gateways, such as those going through firewalls or by VPN.	Policy Procedure Preventive	LAN or WAN environment
Security software should be maintained such that installed software is updated to ensure synchronization with the vendor's most recent versions and updates.	Policy Procedure Preventive	All security programs
Anti-virus and anti-spyware software should be configured to automatically (auto-update) obtain vendor-provided definition files identifying known viruses and spyware.	Procedure Preventive	All Anti-virus software
ITD Requirements		
All agency IT equipment that connects to the Internet through MAGNet must be behind ITD's MAGNet-supported firewall protection.	Policy Standard Preventive	All IT environments
Firewalls should have virus-scanning software installed.	Policy Procedure Preventive	All firewalls
All outside connections from vendors, contractors or other business partners must pass through the ITD-managed firewall.	Policy Procedure Preventive	All MAGNet agencies
Management should ensure that appropriate email filtering and blocking capabilities are employed at the firewall level, including: (a) Blocking all multi-part MIME messages at the gateway, (b) Discarding emails containing files with extensions, that are affiliated with a virus. (c) Disallowing private email that is separate and apart from an agency's primary email system.	Policy Procedure Preventive	All mail gateways

APPENDIX 3

Date of Virus Infection by Agency per ITD

Virus Infection Date	12/28/04	12/15/04	11/19/04	11/19/04	10/29/04	7/8/04	6/30/04	5/1/04	3/22/04	2/25/04	1/27/04	1/23/04	12/22/03	10/31/03	10/9/03
Agency Name / Virus	Randex.CCF	Erkez.D@mm	Sober.I@MM	Femot.Worm	Beagle.AV@m	Spybot	korgo.q	Sasser	Netsky.P	Netsky.C	Mydoom	Slammer	Randex	Mimail	Welchia
Architectural Access Board															
Bureau of State Office Buildings						Y	Y	Y		Y					Y
Commission Against Discrimination								Y							
Commission for the Deaf and Hard of Hearing						Y	Y	Y							
Department of Fish and Game															
Department of Revenue															
Department of Social Services						Y		Y		Y					Y
Developmental Disabilities Administration															Y
Disabled Persons Protection Commission						Y									Y
Division of Career Services & Unemployment Assistance															
George Fingold State Library															
Group Insurance Commission															Y
Human Resources Division						Y									Y
Information Technology Division	Y					Y	Y	Y		Y					Y
Legislative Information Services						Y									
Massachusetts Highway Department						Y		Y					Y		Y
Massachusetts Hospital School															
Massachusetts Office of Travel and Tourism															
Massachusetts Office on Disability						Y		Y							
Massachusetts Rehabilitation Commission	Y					Y	Y	Y		Y					
Massachusetts State Lottery Commission										Y					
Massachusetts Turnpike Authority															
Merit Rating Board															
Municipal Police Training Committee						Y		Y							Y
Newton Housing Authority															
Office of Child Care Services						Y		Y		Y					
Office of Inspector General															
Office of Professional Licensure															
Registry of Motor Vehicles	Y					Y	Y	Y							
State Ethics Commission															
Teachers' Retirement Board						Y									
University of Massachusetts Boston															
Victim and Witness Assistance Board						Y		Y							

The system does not record all instances of virus activity. The viruses recorded on the ITD SAS system are based upon viruses detected through scanning or through notification from individual agencies.

APPENDIX 4

ITD's SAS Reported Security Alerts

Severity	Date	Name
High	01/05/05	W32.Randex.SQ
Medium	12/14/04	W32.Erkez.D@mm
High	12/01/04	Critical Vulnerability in Microsoft Internet Explorer
Medium	11/19/04	W32.Sober.I@mm
Medium	10/29/04	W32.Beagle.AV@mm
Low	10/04/04	W32.Bagz@mm
High	08/16/04	W32.Mydoom.Q@mm
Medium	08/10/04	W32.Beagle.AO@mm
High	07/26/04	W32.Myddom.M@mm
High	07/15/04	W32.Beagle.AB@mm
High	07/08/04	New W32.Sasser.Worm
Low	06/25/04	JS.Scob.Trojan
High	06/02/04	W32.Korgo.R
Medium	05/14/04	Dabber
Medium	05/14/04	Multiple Vulnerabilities in Symantec Client Firewall Products
High	05/01/04	W32.Sasser.Worm
High	04/26/04	W32.Beagle.W@mm
High	04/21/04	W32.Netsky.Y@mm
High	04/16/04	W32.Gaobot.AAY
High	04/16/04	W32.Gaobot.AAY
Medium	03/29/04	W32.Netsky.Q@mm
Medium	03/26/04	W32.Beagle.U@mm
Medium	03/24/04	W32.Netsky.P@mm from 3/22/2004
Medium	03/18/04	W32.Beagle.Q@mm
Medium	03/08/04	W32.Sober.D@mm
Medium	03/03/04	W32.Beagle.J@mm
High	03/01/04	W32.Beagle.E@mm
High	03/01/04	W32.Netsky.D@mm
High	02/25/04	W32.Netsky.C@mm
Medium	02/24/04	W32.Mydoom.F@mm
High	02/19/04	W32.Netsky.B@mm
High	02/17/04	W32.Beagle.B@mm also Known as W32.Alua@mm
Critical	02/11/04	Microsoft Security Bulletin MS04-007 ASN.1 Vulnerability Could Allow Code Execution
Medium	01/15/04	1/27/04 W32/Mydoom@MM, WORM_MIMAIL.R
Medium	12/18/03	YS OCSCIC Cyber Security Advisory Re: Cisco PIX vulnerabilities
Medium	11/18/03	W32.Mimail.J@mm
Medium	11/13/03	New Microsoft Security Bulliten
Medium	11/06/03	Oracle Application Server SQL Injection Vulnerability
Medium	10/31/03	W32.Mimail.C@mm
Medium	10/16/03	Windows New Security Bulletins
Medium	10/09/03	W32.Welchia.Worm
Medium	10/06/03	Cumulative Patch for Internet Explorer (828750)

APPENDIX 5

Information Technology Architecture and Enterprise Standards

Virus detection is identified in ITD's Information Technology Architecture and Enterprise Standards as:

- Virus scanning software must be installed at the Workstation, LAN, WAN and Mail Server levels. ITD also has virus-scanning software at the firewalls.
- The software must be configured to:
    - Periodically scan all files that are stored on physically and logically connected disk drives attached to the computer
    - Automatically scan any file that is copied onto a disk drive from an external source including floppy disks and CD ROM disks
    - Automatically scan any file that is opened by an application such as a word processing or spreadsheet application.
- Virus scanning software and virus signatures must be kept current by incorporating the vendor's most recent versions. Software with auto-update capabilities is strongly recommended.

Norton Anti Virus Corporate Edition is recommended.

Virus Detection http://www.mass.gov/itd/spg/publications/standards/archstan.htm#Security