Steven A. McNamara
Inspector General

Office of Inspector General
U.S. House of Representatives
Washington, DC 20515–9990

MEMORANDUM

TO: James M. Eagen III
Chief Administrative Officer

FROM: Steven A. McNamara
Inspector General

DATE: December 7, 2000

SUBJECT: Audit Report – The Chief Administrative Officer Has Implemented Controls To Guard Against Unauthorized Software Programs (Report No. 00-CAO-07)

This is our audit report on the controls against unauthorized software programs in the Office of the Chief Administrative Officer (CAO). The objective of this audit was to determine whether the CAO had established effective software licensing and virus protection policies and procedures, and programs that ensure compliance with those policies and procedures. We concluded that the CAO has a combination of strong policies and active compliance measures regarding software licensing and virus protection.

In response to our October 10, 2000, draft report, your office concurred with our findings and recommendations. Your November 17, 2000, management response is incorporated in this report and included in its entirety as an appendix. Since the corrective actions taken were appropriate and responsive, we consider the recommendations closed.

We appreciate the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this report, please call Christian Hendricks or me at (202) 226-1250.

cc: Speaker of the House
Majority Leader of the House
Minority Leader of the House
Chairman, Committee on House Administration
Ranking Minority Member, Committee on House Administration
Members, Committee on House Administration

THE CHIEF ADMINISTRATIVE OFFICER HAS IMPLEMENTED CONTROLS TO GUARD AGAINST UNAUTHORIZED SOFTWARE PROGRAMS

I. INTRODUCTION

Summary of Findings

The Chief Administrative Officer (CAO) has established an effective software licensing and virus protection program through the implementation of policies and procedures (i.e. the House Information Security Policies (HISPOLs)) and a system of internal controls that ensure compliance with those policies and procedures within the office of the CAO. In April 2000, the CAO began a rigorous review program to periodically reconcile software installations in the CAO with software licenses purchased. The CAO also established an automatic program to guard against the incidence of viruses on CAO computers. The combination of clear guidance and an active compliance program is a best practice that should effectively limit the risk of unlicensed software and viruses in the office of the CAO.

Background

Most commercial software sold in the United States is protected by federal copyright. When an organization purchases a commercial software package, it receives the right, or license, to use the package while the author or publisher retains ownership of the underlying program code as intellectual property. Some licenses to use software can limit how many machines can run the program while others limit the number of users. Network and concurrent use licenses authorize a specified number of users to access and execute the software at any time. In general, site licenses that authorize use at a single site are being replaced by enterprise licenses that authorize unlimited use in a single organization. Although organizations generally purchase their software and obtain licenses, today's interconnected network environment increases the risk that well meaning users may download, use, and distribute unlicensed software programs from a variety of sources. The Software & Information Industry Association (SIIA) estimates that businesses account for more than one-fourth of unauthorized software use.

Network connectivity also increases the risk of spreading malicious code programs that can damage data, software, and hardware or affect the security of computers and networks. Computer viruses, the best-known type of malicious programs, are spread through electronic mail, sharing infected files or from the Internet. Similarly, computers can become infected with "Trojan-Horse" programs, which are virus-like programs that can provide attackers with the capability to control a computer remotely. The most effective methods to protect personal computers from viruses and "Trojan-Horses" are maintaining current versions of anti-virus programs and requiring users to use software only from known and trusted sources.

HISPOL 002.0, "General Information Security Guidelines for Protecting Systems from Unauthorized Use," dated February 4, 1998, states that it is the policy of the House to comply fully with copyright laws pertaining to computer software. Accordingly, the House prohibits the illegal duplication or use of any software or related documentation. The HISPOL also requires House employees to ensure that "virus protection is in-place, functional, and current." The CAO is charged with the responsibility of ensuring that software packages installed within CAO offices are inventoried and reconciled to House supported software licensing agreements in accordance with HISPOL requirements as well as maintaining current anti-virus protection software within CAO offices.

Objectives, Scope, And Methodology

The first audit objective was to determine whether the CAO had established effective software licensing and virus protection policies and procedures. The second objective was to determine if the CAO had established programs that ensure compliance with those policies and procedures. The review of software licenses was limited to programs installed in January 1997 or later. House policies on record retention did not require House offices to maintain documentation on software purchases made before January 1997.

The audit coincided with the CAO's first reconciliation of software licenses. The audit scope covered the approximately 600 desktop computers attached to the House network within CAO offices, but did not include any notebook computers or servers on the CAO network. Since this audit was limited to the CAO, we did not assess procedures for software license validation or virus protection in any other House office and cannot address the overall risk of unlicensed software or viruses in the House. We performed the following specific tasks during the review.

- Evaluated the adequacy of House policies, CAO guidance and procedures related to software licensing and protection against unauthorized software and compared House policies against similar policies at other Federal agencies and academic institutions to identify best practices in these areas.

- Reviewed the process and procedures used within CAO offices to document software installed on personal computer desktops and reconcile those software installations to software licenses. This included examining controls over the automated tool used to identify software installed on computer systems (NetCensus), the controls to ensure the integrity of that information, the process used to generate management reports from that data, and the reconciliation process.

- Reviewed software license documentation for a random statistical sample of software installations.

We conducted the review in accordance with Government Auditing Standards *(1994 Revision)* established by the Comptroller General. The Information Systems Audit and Control Foundation's CobiT: *Control Objectives for Information and Related Technology (1998 Edition)* provided general criteria for the management of the software

licenses and virus protection techniques. The CobiT framework is comprised of four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring.

Internal Controls

Controls that prevent unauthorized software installations and the introduction of computer viruses or other malicious code programs within the Office of the Chief Administrative Officer were generally effective at the time of our review. The continued success of those controls will require House managers to maintain their emphasis on software licensing and virus prevention.

Prior Audit Coverage

No prior audits have covered software license compliance and anti-virus protection in the office of the CAO.

II. RESULTS OF REVIEW

CAO Program Effectively Implements House Software Licensing and Virus Protection Policies

The CAO has a combination of strong policies and active compliance measures regarding software licensing and virus protection. Although HISPOL 002.0 addressed both issues in 1998, the CAO issued specific guidance in April 2000 regarding software licensing within the CAO and instituted an active software license compliance program. To minimize the risk of virus contamination, the CAO combined clear HISPOL guidance with automatic updates of virus protection software since late 1998.

Software License Reconciliation Effort Validates Compliance with Copyright Laws. The CAO completed a review of software installed on desktop computers to verify that all installations are covered by valid software licenses. This reconciliation was the first phase of a planned four-phase project. Phases Two through Four, covering notebook computers, servers, and computers not connected to House networks, were completed after field work ended on this audit. The CAO planned to review software licensing every six months.

The CAO began Phase One of its reconciliation program in April 2000 and finished in July 2000. Using network-scanning software, the CAO collected data on the software installed on its computers and used that data to generate reports of the installations for each office. (The reports excluded software products covered by site licenses, such as operating systems, and known freeware products that did not require license purchases.) Departmental managers then reconciled the generated reports with licenses held to determine whether the CAO owned enough licenses for each software product purchased since January 1, 1997. If the number of installations for a particular software product exceeded the number of licenses, the office removed the product from the workstation or

purchased additional licenses. We reviewed the accuracy and reliability of the network-scanning program and controls over the resulting databases and determined that controls were effective to gather complete and accurate data, maintain the integrity of that data, and report the results. We also reviewed the procurement documentation for a sample of CAO software installed on desktop computers and found adequate evidence of valid licenses for that software.

During Phase One, the CAO identified a limited number of circumstances requiring the purchase of additional software licenses. Many of these instances were related to Word Perfect 9.0 needed by Technical Service Representatives to support House offices that used the software. The information gathered in Phase One also provided a baseline database on thousands of software products installed on CAO desktop computers, including several software products still in use from the early 1980's, such as Lotus 123 products. Besides documenting its software inventory, the CAO can also use this data to evaluate the feasibility of various software licensing options.

Daily Virus Software Updates Protect CAO Computer Systems. The CAO installed virus protection software as standard software on CAO desktop computers and established a program of automatic virus protection updates to minimize the occurrence of viruses. Personnel in House Information Resources (HIR) download updated definition files from the Command AntiVirus website to a centrally accessible server automatically on a daily basis. CAO desktop computers then update virus definition files on each computer automatically, without user intervention. This occurs because the standard CAO desktop software configuration contains the Command AntiVirus software with the "Automatic Update" option selected. Automatic updates ensure that the most recent virus definition files are in place to detect the latest viruses on CAO desktop computers. Manual downloads are available if necessary and the HIR Call Center assists any users who experience difficulties with the automatic updates. We believe that automatic virus updates decrease the risk of viruses on CAO desktop computers.

CAO Program Provides Best Practice in Protection Against Unauthorized Software

During this audit, the OIG contacted a number of Executive branch agencies, academic institutions, and corporations to determine best practices in policies and practices related to software licensing. Although many organizations have good policies, most of them had no program to verify software licenses and relied on the individual user or department manager to ensure their software is legally licensed. Therefore, we believe that the CAO's program for software licensing validation, combining active scanning, reconciliation, and high-level management attention, represents a current best practice in this area.

The CAO also requested OIG input regarding how often it should perform a software license validation. The SIIA's "Software Management Guide" states that audits should be conducted regularly and at least annually. After reviewing the CAO program and the SIIA guidance and rationale, the OIG concluded that annual software license validation reviews were more cost effective for the CAO than semi-annual reviews.

During our review, we discussed the following best practices with management.

- The CAO database on software installations and licenses needs complete and accurate data to provide a baseline for follow-on reviews. The SIIA advocates including the following information in the database: product, version, publisher, software serial number, purchase date, user name, user location, hardware serial number, and comments. Although the CAO database does not currently contain all of the listed information, we consider the SIIA recommendation to be a very conservative approach that may not always be warranted. The CAO should evaluate the cost and benefit of obtaining and maintaining any particular purchase or license data items and collect any additional data deemed necessary during the next software license validation exercise. During our validation review, we found a few instances where CAO managers needed to enter additional information into the database. Since this database will form the foundation of future software license validation efforts, complete historical records will save time and effort in years to come.

- House-owned site licenses on several software packages, such as the Windows 95, Windows 98, and Windows NT operating systems, are accessible by any authorized user on House networks. HIR maintains the APPSERVER file server to distribute the software and for HIR and vendor personnel to use as a resource when they need to reload defective Windows systems and configure other hardware, such as printers. As an added convenience, the software and installation keys are also stored on APPSERVER. The accessibility of the operating systems and installation keys could allow a legitimate House user to copy these files for unauthorized installation of the software offsite in violation of site license agreements. In response to our concern, HIR agreed that the Windows installation keys could be removed from APPSERVER. This would prevent the unauthorized installation of those operating systems while leaving the installation files available for use by HIR personnel and vendors.

Conclusion

The CAO has established an effective combination of policies and an active compliance program to prevent the incidence of unauthorized software on CAO computers. We believe that the CAO program of scanning and reconciling software on all CAO computers represents a best practice in this area. In light of the relative lack of problems found on CAO desktop computers, we believe that the CAO should repeat the software scan and reconciliation process annually while maintaining the same degree of high-level management attention.

Recommendations:

We recommend that the Chief Administrative Officer:

1. Scan CAO computers and reconcile software installations to software licenses annually.

2. Identify all necessary purchase and license information for each software installation found on CAO computers and update the software license database to include all the purchase and license information found.

3. Remove the operating system installation keys for the Windows 95, Windows 98, and Windows NT operating systems from APPSERVER.

Management Response

The CAO fully concurred with the recommendations and has completed a full scan of all desktop and laptop computers, reconciled all software licenses for each machine, and entered all information into a database that will be the starting point for future annual scans. Additionally, the CAO has taken action to limit the access to the operating system installation keys for the Windows 95, Windows 98, and Windows NT operating systems on APPSERVER.

Office of Inspector General Comments

The actions taken by the CAO are responsive to the issues identified and satisfy the intent of the recommendations. The CAO's alternative approach to securing the operating system installation keys should effectively prevent unauthorized persons from obtaining those keys. We consider the recommendations closed.

James M. Eagen III
Chief Administrative Officer

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515–6860

MEMORANDUM

To: Steve McNamara
Inspector General

From: Jay Eagen
Chief Administrative Officer

Subject: Response to the Audit Report Entitled "The CAO Is Implementing Controls To Guard Against Unauthorized Software Programs"

Date: November 17, 2000

Thank you for the opportunity to comment on the Audit Report, "The CAO Is Implementing Controls To Guard Against Unauthorized Software Programs." We have carefully reviewed the report's recommendations and concur with each of them. Included below is a brief response for each of the audit recommendations made and the course we have already taken to implement and close each of these recommendations.

Recommendation 1: We recommend that the Chief Administrative Officer scan CAO computers and reconcile software installations to software licenses annually.

CONCUR.
The Office of the CAO completed a full scan of all desktop and laptop computers and completely reconciled all software licenses for each machine. All information was entered into a database and will be used to perform an annual scan. We believe we have taken appropriate action to close this recommendation.

Recommendation 2: We recommend that the Chief Administrative Officer update the software license database to include all necessary purchase and license information for each software installation found on CAO computers.

CONCUR.
All software license information has been updated in the tracking database and will be used as a starting point for future annual scans. We believe we have taken appropriate action to close this recommendation.

Recommendation 3: We recommend that the Chief Administrative Officer remove the operating system installation keys for the Windows 95, Windows 98, and Windows NT operating systems from APPSERVER.

CONCUR WITH ALTERNATE IMPLEMENTATION.
The "Read" access permission for the files that contained key information was removed from the "Everybody" group. Only specific groups of people within HIR with a need for access to this key information will have "Read" access to these files. This change prevents unauthorized personnel from not only reading the keys but also from copying the files to another location. The net effect is the same as moving the keys to another directory with limited access. We believe we have taken appropriate action to close this recommendation.