SOFTWARE MANAGEMENT

EXECUTIVE SUMMARY

Under a task order with the Office of Inspector General, Jefferson Wells reviewed the Commission's software management. Our review found that some controls and best practices have been established, including a configuration management function and the tracking of some software. We commend the Commission for these actions.

The Commission's controls need to be improved to meet accepted criteria (the Capability Maturity Model), and to be in full compliance with applicable laws and regulations. Our testing found numerous instances of unapproved software on Commission computers and file servers. We are recommending that the Office of Information Technology assign responsibility and improve processes for software management.

SCOPE AND OBJECTIVES

Our objective was to assess internal controls for software management. We also assessed the extent of compliance with applicable laws, regulations, and best practices.

During the review, we interviewed and surveyed Office of Information Technology (OIT) and other Commission staff; reviewed relevant documentation and regulations, including software licensing agreements; and performed tests of internal controls over software on desktops, laptops, and servers at Commission headquarters, the Operations Center, and the Annex. We used an automated tool to help perform our tests (Tally Systems' TS.Census License Compliance Suite).

BACKGROUND

Executive Order 13103, issued September 30, 1998, provides guidance on software management by federal agencies. The Order seeks to ensure that agencies and recipients of Federal funds comply with copyright law.

Appendix A contains the text of the Executive Order and other detailed information on applicable laws, regulations, and best practices for managing software.

The Office of Information Technology (OIT) has primary responsibility for overseeing the Commission's information technology program, including software management. Technology issues involving user offices are reviewed by the Information Officers' Council, which consists of senior staff from those offices. Appendix B contains detailed information on the Commission's organizational structure for software management.

User software is normally distributed from network servers to user desktops through the use of Active Directory, a software management tool. Access to the installation servers is restricted to administrators.

If a problem occurs with the Active Directory distribution, an administrator loads the application manually, using the vendor CD. Server software is either downloaded from the vendor, or installed manually from a vendor CD.

The Configuration Management and Quality Assurance Branch (CM/QA) maintains a library of desktop and network software. Other branches within OIT and user offices also keep copies of some software.

The Commission does not maintain formal documentation on software upgrades and change requests. The responsible Commission contractor indicated that changes are requested by emails and discussed at meetings.

License tracking is not centralized in the Commission. License information may be maintained in either an electronic file or hard copy, depending on the software and the organization involved.

Appendix C provides background on a five stage Capability Maturity Model (CMM), which can be useful in assessing an organization's processes for information technology (IT) management, including software.

AUDIT RESULTS

We found that some controls and best practices have been established for software management, including a configuration management function and the tracking of some software. The Commission's controls need to be improved to meet accepted criteria (the Capability Maturity Model), and to be in full compliance with applicable laws and regulations. Our testing found numerous instances of unapproved software on Commission computers and file servers.

Our detailed findings and recommendations are presented below, organized into the following categories: policy guidance; controls; record keeping; inventories; training; contractors; and performance measures.

POLICY GUIDANCE

The Commission has not yet issued a written policy that assigns specific responsibilities for software management. To help ensure effective software management and compliance with regulations, a written policy needs to be developed.[1]

Recommendation A

OIT should issue a written policy on software management that assigns responsibilities for ensuring compliance with laws, regulations, and best practices.

CONTROLS

Automated Tools

OIT indicated that it has recently installed an automated tool to catalog all Commission desktop, laptop, and server computers. It can further improve software controls by installing additional specialized software (such as snapshot, network, and PC tools). This software can image and map Commission computers and the network, and track licensing requirements for software.

Recommendation B

OIT should install automated software management tools.

User Privileges

Currently, user privileges are not audited to help ensure that users are restricted from downloading or installing executable code or other installation packages and software. Granting users privileges beyond what they require for their jobs could lead to security risks or noncompliance with software licensing requirements.

Recommendation C

OIT should audit user privileges and eliminate unnecessary access rights. The need for shared passwords should be evaluated.

[1] OIT indicated that it has developed an IT Policy Governance Framework that monitors the development and review of all IT-related policies.

Software License auditing

OIT does not currently audit compliance with software licenses through tests of Commission computers. As part of this audit, we conducted an audit of software licenses using an automated tool (TS.Census).

The audit covered over 2700 Commission desktop and laptop computers, or approximately 90% of the computers in headquarters and the Operations Center. We also manually inspected the primary Commission server (on which applications are tested before installation on other servers) and gathered limited information from other servers. We provided OIT with a detailed description of our testing and results.

We found a total of 853 installed applications on Commission desktop and laptop computers. Of this total, 523 were not on the OIT-approved software list. In addition, we could not find licenses for 111 applications, based on purchase and other records.

Of the applications that were not approved, at least 30 were Freeware, and 28 applications could be considered suspicious or potentially malicious. A total of 13 applications appeared to exceed the threshold for licenses, which could make the Commission liable for additional costs or subject to legal action. We also found a total of 604 applications on Commission servers that could not be identified as approved.

Recommendation D

OIT should evaluate our test results and take appropriate action, as resources permit, to ensure that only approved software is installed on Commission computers. It should consider periodically performing audits similar to ours.

Manual controls

The responsibility for software management is distributed throughout the Commission. Thus, the adequacy of controls may vary. For example, physical security appears effective in the test lab, which is locked and maintains installation media in a locked cabinet. License records for back-up media management are also well controlled. However, we found many instances of software installation CDs being left in unsecured workspaces in the Operations Center Annex.

During our review, OIT conducted no audits of hardware. The Asset Management Branch within OIT has recently taken over this responsibility.

As stated in the Background, OIT does not maintain documentation on software upgrades and change requests after the basic foundation has been installed. Also, license tracking is not centralized and standardized.

Finally, OIT currently does not have written procedures governing software disposal or a disposal checklist.

Recommendation E

OIT should enhance manual controls for software management (covering physical security of software; hardware audits; tracking of software licenses, purchases, distribution, and change requests; and software disposal procedures, among other issues).

Preventive controls

At the time of the audit, OIT did not make projections for anticipated user growth, which would assist planning for future software purchases. OIT indicated that it has now begun making such projections.

OIT does not produce management reports on compliance with software licenses. OIT records hardware disposal and storage, but does not have standard procedures for these activities.

Recommendation F

OIT should implement preventive controls for software management (such as user growth projections, management reporting on compliance with software licenses, and hardware disposal procedures).

RECORD KEEPING

OIT does not have written policies and procedures for record keeping that adequately manage the approval, use, and safekeeping of software (including UNIX, backup media, Windows, and other desktop software) and software licenses. Written procedures would help ensure that license thresholds are not exceeded, license certifications are available for review, and record keeping is centralized, timely, effective and secure.

Recommendation G

OIT should develop written policies and procedures for record keeping to adequately manage the approval, use, and safekeeping of Commission software and licenses.

INVENTORIES

OIT does not currently perform inventories of software on Commission computers to ensure compliance with software licensing agreements and copyright laws. The Asset Management Branch within OIT has recently been assigned responsibility for hardware and software inventories.

The Commission numbers hardware with a bar-code system and has users sign a form for all computer exchanges. However, significant hardware changes have occurred recently, including the upgrade of most laptops and a number of servers.

Recommendation H

OIT should perform periodic physical inventories of tracked software installations and hardware, and follow-up as appropriate.

TRAINING

Commission and contractor staff are required to take an on-line course in security and copyright law. The training does not reference specific Commission policies or procedures, and is not tailored to specific groups (*e.g.*, administrators, contractors).

As of July 2004, 94% of the target audience of approximately 4500 staff had taken the course. A total of 261 staff had not started the course and 28 had only partially completed it (90 of these are contractors).

Based on our survey of 40 Commission staff (including IT Specialists, OIT Liaisons, and members of the Information Officers' Council), awareness and understanding of Commission software policies can be improved.

Users with administrator rights need more detailed guidance and training than other users, tailored to their job responsibilities. Currently, specialized guidance and training is not provided to these users. This training could cover copyright protection for software; troubleshooting and security procedures; and detection and reporting of inappropriate activities on computers.

Similarly, contractor staff would benefit from additional training, given OIT's extensive use of contractors to perform sensitive duties (for example, purchasing and handling of software).

Recommendation I

OIT should ensure that all staff and contractors receive and are evaluated on the required training in security and copyright law. OIT should also consider developing specialized training for certain users (such as administrators and contractors).

CONTRACTORS

Commission contractors are not following the same procedures for software purchasing, installation, storage, and license monitoring. Also, procedures for distributing software and computers to contractor staff have not been developed. Consistent procedures for contractors would help provide better software management.

Recommendation J

OIT should develop procedures applicable to contractor acquisition and management of Commission software and hardware.

PERFORMANCE MEASURES

OIT has not developed performance measures for reporting of software licensing information to senior OIT management and appropriate follow-up. These measures would help enhance software management.

Recommendation K

OIT should develop reports for senior OIT management that contain performance measures for monitoring and follow-up on software licensing information.

At a minimum, the performance measures should include a count of current licenses versus the number of installed products; periodic reporting on when software licenses will expire; projected growth areas; and software products being proposed, tested, or evaluated.