149659

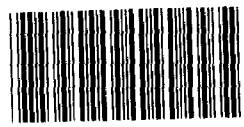
GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-253782

June 30, 1993



The Honorable Jack Brooks
Chairman, Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

This letter responds to your October 8, 1992, request and subsequent discussions with your staff that we review the use of copyrighted personal computer software at the Department of Justice. Specifically, our objectives were to determine (1) the adequacy of the Department's policies and procedures for ensuring the proper use of copyrighted software, and (2) the extent to which unauthorized software exists at Justice agencies in the Washington, D.C., metropolitan area.[1]

To address these objectives, we selected a random sample of Justice organizational components located in the Washington metropolitan area. We also reviewed software management policies and procedures issued by Justice and its components. We used an automated tool to determine the software found on each of the personal computers at the selected components. We then compared the results with licenses and other documentation supplied by Justice to identify any unauthorized software. However, the results of our software audit were compromised during the course of the review. Therefore, we were unable to determine the extent of unauthorized software use at Justice. The enclosure details our objectives, scope, and methodology.

[1]We define unauthorized software as those copies of copyrighted software for which there is no documentation indicating the software is being used in compliance with licensing agreements.

357476/149659

BACKGROUND

Most commercial software is protected by copyright. The copyright owner has the exclusive right to reproduce and distribute copyrighted materials. Copyright infringers can be held liable for violating the copyright. When an agency procures a commercial software package, it usually purchases only the right, or license, to use the package. Ownership of the underlying program code usually remains with the author or publisher. Commercial software, however, can often be easily copied and shared, in violation of licensing agreements. As a result, agencies must establish appropriate policies and procedures to prevent such unauthorized use.

The Department of Justice had about 57,000 personal computers (PCs), distributed nationwide among 32 organizational components as of January 31, 1993. Our review focused on the approximately 19,000 PCs at Justice components located within the Washington, D.C., metropolitan area, along with Departmentwide policies and procedures.

RESULTS IN BRIEF

Policies and procedures issued by Justice at the Department level and most of its components are not adequate since they do not address the protection of copyrighted software. We were unable to test the extent of Justice compliance with software copyrights, however, because agency components became aware of the purpose of our audit and may have corrected deficiencies in advance of our visits. Agency officials nonetheless agreed with our assessment of the inadequacy of their policies and procedures, and plan to take corrective action.

POLICIES AND PROCEDURES DO NOT ADEQUATELY ADDRESS COPYRIGHT ISSUES

Departmentwide policies and procedures regarding software management are generally contained in computer security guidance and, for the most part, focus on the issue of virus protection. Most component-level policies and procedures we reviewed do not address the issue of software licenses and copyright protection; those that do address these issues do so to varying degrees. For example, the Drug Enforcement Administration (DEA) specifically states that ". . . copying, duplicating, or other distribution of software for other than backup use

by the lawful users is not allowed . . ." and explains that any DEA employee who makes an unauthorized copy or alters commercial software is legally liable for copyright violations. According to the Office of Intelligence Policy and Review, "the security manager shall ensure that software loaded on the system is authorized and has been checked for viral infection and that copyright laws shall be adhered to."

Justice officials confirmed that the Departmentwide software policies and procedures were principally designed to protect against the introduction of computer viruses to PCs, not to provide copyright protection or comply with licensing agreements. According to them, copyright issues have not received extensive management attention at the Department level and are therefore not incorporated in its policies and procedures.

These officials indicated that, as a result of our review, ongoing revisions to Departmentwide guidance and future Justice systems compliance audits will cover software licenses and copyright protection issues.[2] Revisions to policies and procedures are to be made final in the next 6 months.

EXTENT OF UNAUTHORIZED SOFTWARE USE IS UNKNOWN

As mentioned, we were unable to determine the extent of unauthorized software use at Justice because the audit was compromised. The confidentiality of the scope and methodology of our review was imperative to its success. We worked with central management offices at Justice to limit the extent to which specific audit objectives were made known. Justice memoranda notifying agency components of our visits were consistent with our agreements with management and did not mention specific objectives. During the course of the audit, however, it became apparent that the personnel at the sites we reviewed were aware of the purpose of our visits and may have corrected deficiencies. Specifically, we obtained a memorandum in which DEA management informed its staff of our site visits and instructed office heads to

---

[2]Justice compliance audits are reviews by the Department's computer and telecommunications security staff to determine compliance with Department and governmentwide policies for using computers and telecommunications equipment.

> "review all published policies and procedures regarding the utilization and security of microcomputers in your offices, especially those provisions regarding what software may be legitimately installed and utilized on DEA microcomputers. If you find any deficiencies, please correct these at the earliest possible time."

As a result of this memorandum, we cannot be assured of the credibility of the results at the sites we visited, or the locations we planned to visit later. Therefore, as agreed with your staff, we terminated our review of specific Justice sites.

At the two sites where we completed our visits before terminating this portion of our review, we identified few instances of unauthorized software. We identified 527 copyrighted software packages on 91 PCs located at Justice's Washington Data Center, in Rockville, Maryland, and DEA's Network Operations Center, in Arlington, Virginia. Justice personnel provided documentation showing compliance with license agreements for all but five of 443 copyrighted software packages identified at the Washington Data Center. At the Network Operations Center, DEA personnel provided documentation for all of the 84 software packages on 18 PCs.

CONCLUSIONS

The lack of adequate policies and procedures exposes Justice to increased risk that unauthorized software use will occur. Such unauthorized use infringes upon the rights of copyright owners and deprives them of legitimate profits. Justice's proposal to include copyright protection issues in its policies and procedures and to monitor adherence to these policies in systems compliance audits demonstrates, however, appropriate management attention to this issue, and is a good first step toward reducing this risk.

- - - - - -

We discussed the facts in this letter with Justice officials, and have incorporated their comments where appropriate. However, in accordance with your wishes, we did not obtain written agency comments on a draft of this letter. We conducted our work from December 1992 to May 1993, in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. We will then give copies to other interested parties. Copies will also be made available to others upon request.

Please contact me at (202) 512-6406, or Linda Koontz, Assistant Director, at (202) 512-7487, if you have any questions.

Sincerely yours,

Jack L. Brock
Director, Government Information
and Financial Management

OBJECTIVES, SCOPE, AND METHODOLOGY

In October 1992 the Chairman, House Committee on the Judiciary, requested that we conduct a governmentwide investigation into the unauthorized use of copyrighted personal computer software by federal agencies. Further discussion with the Chairman's office led us to focus our review on Department of Justice locations in the Washington, D.C., metropolitan area.

To determine how copyrighted software is used at Justice, we requested (1) copies of applicable policies and procedures for software management and (2) agencywide data on the number of personal computers in use, by organizational component and location. As of January 31, 1993, Justice had about 57,000 PCs nationwide, with about 19,000 in the Washington, D.C., metropolitan area.

We reviewed policies and procedures for software management issued at the Department level and by individual agency components. We discussed these with Justice officials responsible for their development and enforcement.

To determine the extent of unauthorized software use in Justice's Washington area offices, we chose sites at random from among the 195 offices having control of about 19,000 personal computers. Using random numbers, sites were selected such that locations with large numbers of PCs were more likely to be chosen than locations with smaller numbers of PCs.

We used the software management tool SPAudit, version 2.8, to determine the specific software programs contained on the PCs we audited.[3] SPAudit identifies hundreds of the most common software programs by searching for a unique file name ("identifier"), which it associates with a particular software program. We revised the software by adding identifiers for new software and eliminating identifiers that were not unique

[3] SPAudit was developed by the Software Publishers Association (SPA) and is the tool SPA has used to conduct software audits of businesses throughout the United States since 1988. It is a software program that searches the hard disks of personal computers for popular programs, to provide an inventory of the software currently installed on the PC.

to one software package. In addition, we worked with representatives from Justice and the National Institute of Standards and Technology to analyze the SPAudit source code to ensure that it performed as intended and only read file names, not the contents of the files.

SPAudit provided a report listing the software product, product publisher, product identifier, and the number of copies found on each PC. We reconciled these data with systems disks, purchase receipts, and other documentation provided by Justice and DEA personnel to establish the authorized number of software copies.

(510911)