Audit of the Software License Compliance

Audit #00-09

Prepared by
Office of Inspector General

Allen Vann, Inspector General
John Lynch, Lead Information Systems Auditor

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

3301 Gun Club Road, West Palm Beach, Florida 33406 • (561) 686-8800 • FL WATS 1-800-432-2045 • TDD (561) 697-2574
Mailing Address: P.O. Box 24680, West Palm Beach, FL 33416-4680 • www.sfwmd.gov

MGT 08-06F

November 17, 2000

Audit Committee Members:
Mr. Mitchell W. Berger, Chairman
Mr. Gerardo B. Fernandez, Member
Mr. Patrick J. Gleason, Member
Mr. Nicholas J. Gutierrez, Member
Mr. Michael D. Minton, Member
Mr. Harkley R. Thornton, Member
Ms. Trudi K. Williams, Member
Mr. John Fumero, Ex Officio

Re: Final Report-Audit of the Software License Compliance, Audit #00-09

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. The audit focused on assessing the District's compliance with licensing requirements for computer software used on our computers. This report was prepared by Mr. John T. Lynch, Lead Information Systems Auditor.

Sincerely,

Allen Vann
Inspector General

AV/jl
Enclosure

c: Frank Finch
James E. Blount
Jock Merriam

- TABLE OF CONTENTS -

INTRODUCTION

This audit reviews the Information Technology Division's (ITD) effectiveness for controlling software usage at the District. In each of the past four fiscal years the District has budgeted over a million dollars per year for software related purchases. In Fiscal year 2001 the amount budgeted has nearly doubled. The audit was conducted pursuant to our approved annual audit plan.

BACKGROUND

Over the past five years the District has budgeted almost $7 million dollars for computer software license fees. These funds are used to purchase computer software for the District's computers.

SFWMD: Computer Software License Fees

Budget Year	Amount Budgeted
1997	$1,096,156
1998	1,019,329
1999	1,200,487
2000	1,281,357
2001	2,227,742
Total	**$6,825,071**

Pocurement of Programming Services for Completion of Solicitation Contractual Agreements for Computer Software Licensing Fees.

There are over 16,000 different executable program files representing nearly 1000 licensed software packages distributed over the District's personal computers (PC's), Unix Workstations, Unix Servers and Digital Equipment Minicomputers. Because of strict anti-pirating laws, records should be readily available to provide evidence that all software products used on District computer systems have been legally purchased, properly distributed, and managed within the limits of the license agreements for their use.

The issue of controlling & accounting for software and the avoiding the use of unlicensed (pirated) software is universal. It is a global problem for software users that can result in significant liability.

Therefore, it is incumbent upon the District, as the purchaser of licensed computer software products, to maintain control of the original software media (disks or CD-ROM) and retain proof of purchase and/or any license agreements. Computer software used on a computer where proof of purchase cannot be provided is considered an unauthorized copy or "pirated" software. Using "pirated" software can result in both civil and criminals penalties against an individual or organization that has title to the computer system. [1]

[1] *The BSA Guide to Software Management*. Business Software Alliance. Retrieved September 2000 from the World Wide Web: http://www.bsa.org

Federal copyright law automatically protects software. The rights granted to the owner of a copyright are covered in the Copyright Act, Title 17 of the United States Code. The Act gives the owner of the copyright "the exclusive rights" to “reproduce the copyrighted work" and "to distribute copies ... of the copyrighted work" (Section 106). It also states that "anyone who violates any of the exclusive rights of the copyright owner ... is an infringer of the copyright" (Section 501). Several penalties for violation of copyright law are set forth in the Code. United States law allows up to 5 years in jail or fines up to $250,000 or both for the distribution of 10 or more copies of software with a total retail value exceeding $2,500. Software copyright owners can also bring civil action including "stop use" (injunctive relief) and "monetary awards" (damages) under current United States law. [2]

The District is liable for violations by its employees. Therefore, it is very important to have appropriate computer software policies, standards, guidelines, and procedures implemented and understood by all employees.

In December 1997 the Federal No Electronic Theft (NET) Act became law. The NET Act strengthened the copyright and trademark laws, closed some loopholes in criminal copyright and trademark provisions, and provided enhanced protection of digital information by amending Title 17 (Copyright Law) and Title18 (Crimes and Criminal Procedure).

It should be noted that the Act states in Title 17, section 501 that:

> *"anyone" includes any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this title in the same manner and to the same extent as any non-governmental entity.*

There is no exception from the law for State government or it's employees.

[2] *Piracy and US Law.* Business Software Alliance. Retrieved August 2000, from the World Wide Web: http://www.nopiracy.com/swandlaw_c.html

OBJECTIVE, SCOPE & METHODOLOGY

The objectives of this audit were to confirm that all software used on District computers were: purchased, properly accounted for and licensed. In conducting this review the following steps were taken:

- reviewed the District's Computer Data and System Security Policy,
- reviewed current laws and regulations regarding software use and licensing,
- sampled District software records and license agreements for software currently in use,
- interviewed Information Systems personnel responsible for software purchasing and licensing,
- gained an understanding of the process of purchasing, distributing and removing of licensed software for and from District computer systems, and
- evaluated the effectiveness of Information System's use of a specialized software program in monitoring and controlling software loaded onto District computers.

Our audit was performed in accordance with "generally accepted government auditing standards" as promulgated by the Comptroller General of the United States. Fieldwork for this audit was conducted intermittently between February 2000 and September 2000.

FINDINGS AND RECOMMENDATIONS

Summary

In order to properly control the use of computer software, it is necessary to maintain records of purchases, license agreements, and the number of software packages in use. In February 2000, the Computer Systems and Support Department designated a staff person as "Software Compliance Associate" to accomplish this. However, because of the large number of software packages owned by the District, little progress has been made.

There are over 650 different computer programs that have been purchased/licensed just for the District's personal computers. Of these computer programs, we found that documented compliance files have been "completed" for only 43 programs. In our review of these 43 files, we found that there were:

- Inconsistencies in the number of products in use and the number purchased/licensed,
- Insufficient proof of purchase, and
- Missing copies of Licensing Agreements.

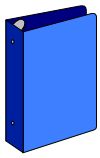
Based upon current practices, we have concluded that there is no assurance that the number of copies of software currently in use does not exceed the number of authorized copies. Similarly, individual computers are not adequately monitored to ensure that unauthorized or illegally obtained software has not been loaded onto District computers. Unauthorized copies of computer software can result in financial penalties and loss of public confidence in the District's management of its resources.

The District's current information systems policy is outdated. The approval of the replacement *draft* policy, which addresses the issue of software compliance, is overdue.

Management agreed with our recommendations and stated:

"The task of documenting what software exists on every computer and matching products with valid software licenses or purchase orders is labor intensive and may also become very costly. However, we agree that we must take immediate action to step up our efforts for bringing the District into compliance."

Draft District Policy
Needs To Be Issued



The District policy for information technology (Computer Data and System Security, Policy #17.01000) has not been revised since the initial implementation of the policy in 1990. This policy does not address some of the current technological issues and organizational changes.

In a study prepared for the Software Business Alliance (September 1999) it was reported that 93% of the companies with a software usage policy in place feel that the policy has been effective (in "reducing or preventing software piracy"). These companies reported that the top challenges with a policy were implementation, enforcement and educating employees.[3]

The District has drafted a revised "information systems policy package". However, this new policy has not reached the point of final review and approval for implementation. In our 1998 *Audit of the District's Information Systems Security* (Audit #98-03), we recommended the completion and issuance of the revised policies package. While management agreed with the recommendation, the policy has still not been issued/implemented.

The proposed new draft policy consists of separate policies, standards, and guidelines that address more current issues of software usage such as:

Information Systems Security Policy:

> Software shall be reviewed, evaluated and approved for scheduled installation. To prevent infection by computer viruses, employees must not use any software on District-owned hardware not first tested and/or approved by the Information Technology Department.
>
> Software used on District information systems shall be licensed to the District by the appropriate legal party.
>
> Employees who knowingly copy or use software other than as authorized by the licenses owned by the District shall be subject to corrective action for theft of District property in accordance with the Corrective Action Policy (03.603). This

[3] *Software Management Study*. (September 1999). Yankelovich Partners for the Software Business Alliance.

includes unauthorized copying of or use of District software on District or non-District information systems.

Information Security Standards:

A user may not intentionally and knowingly use, copy or store purchased software on District computing or communicating facilities in violation of copyright laws or license agreements

Information Security Guidelines:

It is an infringement of District policy to copy proprietary software in violation of a licensing agreement.

Subsequent to issuance all District staff should be notified and trained on the new policy, standards and guidelines.

Recommendations

1. **Finalize and implement the draft information system policy, standards, and guidelines.**

   Management Response: Management agrees with the recommendation. Our current policy is dated and should be revisited. We believe this policy should not be included as a part of the Information Technology security policy, but should be a stand-alone policy on software compliance. As such, it would fit well as part of an overall policy or standard relating to the use of District owned equipment.

   The recommendation can be satisfied by creating a new software compliance policy and following proper District processes for approval and publication.

   Responsible Division: Information Technology

   Estimated Completion Date: December 1, 2000

2. **Educate all employees on District's computer software policy and the penalties associated with using unlicensed (pirated) copies of computer software on District computer systems.**

Management Response: We fully agree this recommendation is an integral part of the software compliance effort.

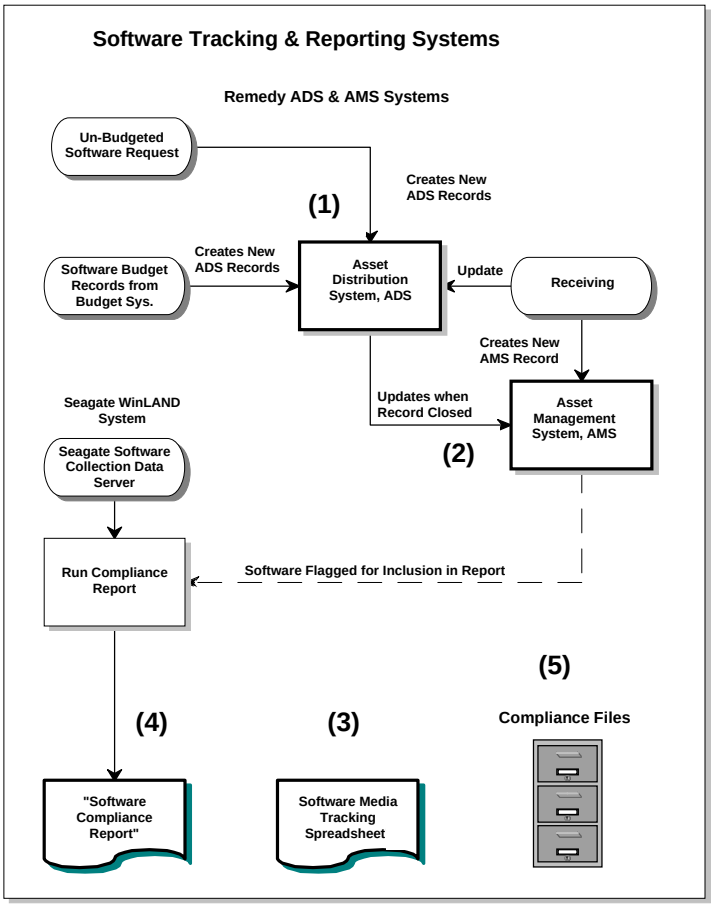
We intend to satisfy this recommendation by holding a series of educational meetings for all employees to promote compliance awareness. Special sessions for Division and Department Directors will also be held focusing on their roles and responsibilities in this effort. Additional advertising methods will include pages posted on the I-Web, posters, paycheck inserts, and group e-mails.

Responsible Division: Information Technology

Estimated Completion Date: December 15, 2000

District Software Tracking System Could Be Improved

The control process for licensed software starts with the budget process. The Fiscal Year 2001 proposed District budget for "Computer Software License Fees" is $2.2 million.



Upon approval of the budget, Information Technology Division's Computer Systems & Support Department will initiate software procurement and compliance administration. Budget software funding is downloaded after the budget is approved into the Asset Distribution System (ADS). In addition, records are generated in this system during the year as unbudgeted software requests are approved. (See (1) in the chart to the right).

When software is received and installed the Asset distribution records are closed and records are generated in the Asset Management System (AMS). (See (2) in the chart). The AMS is then used to track each installed software package.

The original copy of software media (CD, Disk or Tape) is kept in the ITD vault located in the B-50 building and is tracked on an electronic spreadsheet. (See (3) above). The vault is protected with a combination lock and alarm. The media files within the vault are secured in a locked cabinet.

The information contained in this physical inventory spreadsheet consists of:

- Product Name,
- Version,
- Number of Copies,
- Location in Vault (file #), and
- Media Type.

The database used to manage an organization's software holdings should contain as a minimum:

- *Software publisher, title, version and serial number,*
- *Location of where original license and original media are stored,*
- *User(s) name, contact details and location,*
- *Asset number of machine where software is loaded,*
- *Name of installer and date of installation.*[4]

By combining the information on the physical inventory spreadsheet with the AMS database, the District could establish a "software holdings database" in AMS. This would provide a single source for information on the disposition of each software package and eliminate the need for the spreadsheet.

The Information Technology Division's Computer Systems & Support Department uses a separate program (WinLand by Seagate) that keeps track of software used on computers at the District. (See chart (4) on previous page). Every time a computer connected to the District's network is restarted this software tool scans the hard drive for data about all executable program (.exe) files. There are over 16,000 entries for .exe files found in the WinLand data collection file. Utilizing this data, the WinLand program can generate reports about the name, location, and the quantity of program files found on each users system.

A hard copy of the actual purchase order, license agreements and registration cards for each software product should be kept in the compliance files that are currently under development. (See chart (5) on previous page). The "hard copy" file should be cross-referenced to the AMS database.

[4] Silltow, John. (1999). *Software Management Processes*. Retrieved September 1999 from the World Wide Web: http://www.itaudit.org/forum/software/f217so.html

Recommendations

3. Information on tracking the location of the original copy(ies) of the software media should be incorporated in the AMS database.

Management Response: Management agrees with this recommendation. The Asset Management database will be modified to record the location of the original software media and to track the destruction of excess originals.

Every attempt will be made to capture past information and update records. However, because of prior purchasing decentralization throughout the District, complete historical reconciliation may not be available. Discrepancies in the reconciliation will be dealt with appropriately**.**

Responsible Division: Information Technology

Estimated completion date: December 15, 2000

Compliance Files Need to Be Completed And Reconciled To Purchasing Records

A project was initiated in February 2000 with the establishment of a "Computer Compliance Associate" position in the Computer Systems and Support Department to inventory the software packages that have been loaded on all District computer systems. This includes Personal Computers (PC), Unix Workstations (UNIX), Macintosh Computers (Mac), and the Digital Equipment Corporation (DEC) systems. There are more than 650 software packages for the PC's alone. Work has not started on UNIX and MAC software. Only forty-three compliance files have been completed to date.

SOFTWARE COMPLIANCE

Software Compliance is responsible for receiving, recording and maintaining all District software media and records. This group installs and configures software to be compatible with District specific infrastructure. They design and develop necessary software compliance reports utilizing a proprietary Boolean query language. In addition to this they also, create and modify records in the District's Asset Management Database.

SERVICES

- Design and development of software compliance reports.
- Install, configure, and test for software upgrades on Client PC's.
- Install, configure, and test new software packages on Client PC's.
- Maintain media to ESD and HVAC industry standards & procedures.
- Provide ad hoc reports to aid decision-making software purchases & upgrades.
- Provide routine reports for software upgrades.
- Track and monitor all District installed software using polling software

EMPLOYEES

- Contact: Kim Teel
- Service Employees

Source: District IWEB page
Computer Systems & Support

We reviewed the 43 "completed" compliance files for PC software. In our review we looked for (a) *proof of purchase* and (b) a *copy of the software license*. Proof of purchase could be a purchase order, procurement card receipt, registration card with serial number, or a letter from the vendor stating the number of copies licensed to the District. The software license should be a copy of the actual license agreement that states the conditions and terms of use for the particular software package. This agreement could be in the form of an *individual*, *floating*, *concurrent*, or *site* license.

The review of the 43 "completed" compliance files revealed the following:

- There are 19 cases (44%) where the number of reported software packages supported by actual *proof of purchase* does not agree with the receipts found in the file. Of these 16 are overstated and 3 are understated.

- There are 10 cases (23%) where the quantity reported in use exceeds the number of software packages reported as purchased in the file.

- There are 24 files (56%) that do not contain *a copy of the software license agreement*.

Recommendations

4. Compliance files must contain adequate documentation to support the current use of software on District computers.

Management Response: Management agrees with the recommendation. According to the Certified Software Manager Course Manual produced by the Software Publishers Association, Section 5, page 5-2:

"SPA considers a software application unauthorized if ownership cannot be substantiated with documentation that proves proper license. Documentation may include the following:

Dated invoices, purchase orders, and/or receipts showing the product(s) and quantity purchased; or

Dated software or hardware reseller reports itemizing the products(s) and quantity purchased"

Based on this information, being able to produce the purchase orders for specific software packages is sufficient proof of license compliance.

We will make every attempt to locate license agreements or purchase orders and take appropriate action for any software copies that documentation cannot be found.

Purchase order information for each software package received will be logged in the Remedy system (automatically updating the Asset Management System) enabling us to produce a listing of purchase orders for a specific product upon request.

Responsible Division: Information Technology

Estimated Completion Date: June 1, 2001

5. **Starting with all newly purchased software, compliance files for all District software needs to be maintained and reconciled against the Asset Management System (AMS) and Software Compliance Reports.**

Management Response: Management agrees with the recommendation. All newly purchased software is currently being recorded in the Asset Management System. From the Asset Management System we are able to produce a list of purchase order numbers for any specific software package. Copies of the listed purchase orders can be produced and will serve as proof of purchase according to the Software Publisher's Association (SPA).

It is our intent to modify the current software compliance report to improve accuracy. The current reconciliation process will be reviewed for improvements and changes implemented immediately.

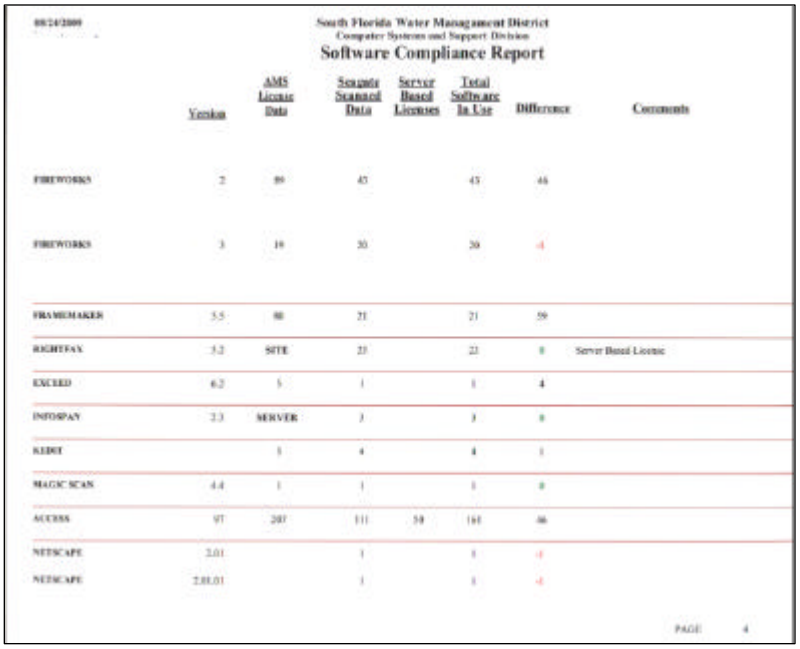
Responsible Division: Information Technology

Estimated Completion Date: December 15, 2000

Compliance Reporting Needs to Include All Software And Be Reconciled to AMS Records

It is important to collect software compliance information and report any violations on a regular basis.

Currently a compliance report is generated using the data collected by the WinLAND monitoring program and the Remedy Asset Management System (AMS) database. Only the information for the 43 "completed" software packages was flagged in AMS for inclusion in Software Compliance Report.



South Florida Water Management District
Computer Systems and Support Division
Software Compliance Report

	Version	AMS License Data	Seagate Scanned Data	Server Based Licenses	Total Software In Use	Difference	Comments
FIREWORKS	2	89	45		45	44	
FIREWORKS	3	19	20		20	-1	
FRAMEMAKER	5.5	80	21		21	59	
RIGHTFAX	5.2	SITE	23		23	0	Server Based License
EXCEED	6.2	5	1		1	4	
INFOSPAN	2.3	SERVER	3		3	0	
KERIT		3	4		4	1	
MAGIC SCAN	4.4	1	1		1	0	
ACCESS	97	207	111	50	161	46	
NETSCAPE	2.01		1		1	-1	
NETSCAPE	2.01.01		1		1	-1	

PAGE 4

Our review of the compliance report for these 43 software packages revealed the following:

- 9 software packages (21%) were found to be in use where the quantity being used exceeds the number of copies reported by the AMS system.

- 21 differences (49%) were found in the number of copies reported in the AMS system and the number of copies reported in the compliance files. Of these AMS overstated 11 and understated 10.

- 13 software packages (30%) are currently in use where the number of packages being used exceeds the number of receipts found.

These 43 files for PC software compliance only represent a fraction of the nearly 1,000 software packages loaded on the District's PC's, Unix Workstations, Unix Servers, and DEC minicomputers. There are hundreds of software packages whose program files (.exe) have been scanned and reported on the WinLand server that have not been reviewed. Some of these software packages could be unlicensed.

Recommendations

6. **Where the Software Compliance Report reveals that more copies of a product are in use than purchase records support, the Computer Systems & Support Department should take steps to immediately remove excess software or (if deemed appropriate) purchase additional licensed copies.**

   Management Response: Management agrees with the recommendation. In instances where software compliance violations are found, the CSS Department shall inform the computer user and the user's Director or Supervisor. The Director shall determine whether the software is justified or whether it should be removed. If the computer user needs the software, the CSS Department will purchase required licenses.

   Responsible Division: Information Technology

   Estimated Completion Date: June 1, 2001

7. **The Software monitoring tool WinLand should not only scan the files, but should generate an exception report on a regular basis of all program files (beyond known District software products) to determine if unlicensed software is being loaded on District computer systems. Improperly loaded software should be removed and corrective action taken.**

   Management Response: Management agrees with the recommendation. WinLand is not capable of this level of reporting. CSS will attempt to identify another product that has these capabilities and determine the feasibility of purchasing it to implement this recommendation.

   Responsible Division: Information Technology

   Estimated Completion Date: March 1, 2001