Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

Strengthening VETS' Software Management Controls Can Prevent Unauthorized Software Use and Potential Software Piracy

FINAL REPORT

Report Number: 23-01-014-02-001
Date Issued: September 28, 2001

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) conducted an audit of the Office of Veterans' Employment and Training Service (VETS) to determine whether VETS has the proper procedures in place to help ensure computer software products are not used in violation of copyright laws, and whether unauthorized software exists on the agency's computers. The audit was conducted in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States.

Our audit found that 35 copies of software applications were unauthorized (***see Attachment A***).

OIG attributes these problems to multiple platform system configuration, lack of employee awareness and understanding, employee-owned software introduced by employees, and not having an appropriate record-keeping system.

We recommend the VETS' Assistant Secretary initiate the following corrective measures to improve the agency's software management:

1. Remove all unauthorized software applications identified by our audit.

2. Fully implement WindowsNT system configuration during the next fiscal year to cover the entire VETS' organization, or assist VETS in developing procedures to manage software over a multiple platform system configuration.

3. Communicate (e.g., *VETS' Alert*) on a regular basis to make VETS' employees aware of the importance of using only authorized software.

4. Work closely with the Chief Information Officer (CIO) and the Office of the Assistant Secretary for Administration and Management's (OASAM) Information Technology Center (ITC) Director for ensuring that explicit software requirements are developed to meet VETS' needs.

5. Assign responsibilities for the purpose of developing a software inventory and a record-keeping system design to identify all software product purchases and related license agreements.

6. Develop and maintain on a continuing basis an updated list of all authorized software used by VETS by performing periodic inventories of software.

- - - - - - - - -

Based on the response to the draft report, and the planned corrective actions, the OIG has resolved all of the above recommendations and will continue to work closely with your office to bring each to closure.

BACKGROUND

Software piracy occurs whenever a software program is downloaded and/or installed, run, or copied without a proper license from the software manufacturer.

Software vendors attempt to control the unauthorized use of their products through license agreement provisions. The license agreements are protected by Federal copyright statutes. The specific license agreement for each software product is explained in documentation accompanying the system installation and program diskettes. License agreements specify that each software program purchased is to be used on one computer at a time, at a site, or on a Local Area Network (LAN).

One way in which software piracy can occur is if Department of Labor (DOL) employees bring software applications from home or by downloading it from the internet. In order for DOL agencies to control and prevent software piracy, there must be a process in place for identifying what the agency owns and what is allowed to be installed on government computers. Executive Order (EO) 13103 encourages the preparing of software inventories and a determination of what software is authorized for use.

OASAM operates the Employee Computer Network (ECN) which is used by VETS. Hardware and software that are to be used on a network Personal Computer (PC) workstation that is directly or indirectly connected to or will access an OASAM operated LAN is required to be certified by OASAM's ITC. OASAM is responsible for the core load of software installed on the ECN. However, VETS can request OASAM to certify and install software applications purchased by VETS for use on the network. In this case, the two agencies (OASAM and VETS) share some responsibilities in the area of software management since the software is owned by VETS, but certified and installed by ITC.

There are multiple operating system platforms as part of VETS' system configuration throughout the agency based on a sample of 50 computers. There is WindowsNT with or without administrative rights, Windows98, and Windows95.

OBJECTIVE, SCOPE, METHODOLOGY AND CRITERIA

OBJECTIVE

The objective was to determine whether VETS has the proper controls and procedures in place to help ensure computer software products are not used in violation of copyright laws, and whether unauthorized software exists on the agency's computers.

SCOPE

The audit was conducted in VETS' National Office and selected regional and state offices.

We scanned a total of 50 computers consisting of 12 desktop computers in the national office and 38 desktop computers throughout selected regional and state offices. Computers in the national office were selected based on a random statistical sample. We scanned all (100%) computers found in the regional and state offices cited in the scope section above.

The audit covered the period of May 15, 2001 through August 21, 2001. An exit conference was held on July 12, 2001.

METHODOLOGY

OIG used a software tool developed by Attest System, Inc., titled GASP 5.2 to audit VETS' computers. Using this tool, OIG performed a scan of 50 desktop computers in VETS to detect whether unauthorized software was installed on the computers. This software is loaded on the computer by inserting the audit disk in the computer's floppy drive. As the program is executed, it searches for all files containing programed instructions associated with software applications. The reporting module of GASP comes with a Software Identification Database (SID) which allows it to identify which applications were found and its related information such as publisher, version and title. The SID does not have a record for every software ever published worldwide. Therefore, if a program file is found and it is not recognized by the SID, the report classifies this as unidentified software. Upon completion of the scanning process, analyses were performed to identify unauthorized software products.

Our assessment was limited to policies and procedures covering internal controls relative to copyright/licensing requirements and what has been officially authorized to be installed on the individual PCs.

CRITERIA

The primary policies guiding this audit are the GAS issued by the Comptroller General of the United States, U.S.C. Title 17, EO 13103, and the Department of Labor Manual Series (DLMS-9) Chapter 1200.

U.S.C., Title 17, section 504 states that a civil action may be instituted for injunction, actual damages, or statutory damages up to $150,000 per infringement.

EO 13103 relating to computer software piracy states that it shall be the policy of the United States Government to work diligently to prevent and combat computer software piracy to prevent the violation of applicable copyright laws.

FINDING, CONCLUSION AND RECOMMENDATIONS

We found that VETS follows DLMS-9 Chapter 1204, and has addressed computer security in its Security Program Plan and Standard Administrative Guidance. However, there is still a need for VETS to strengthen its management controls over software to prevent the use of unauthorized software products and the potential for software piracy.

FINDING

UNAUTHORIZED SOFTWARE EXISTS IN VETS

OIG found a total of 35 copies of unauthorized software while reviewing a sample of 50 computers **(see attachment A).** Thirty-two copies of unauthorized software were found in the four regional and five state offices visited and three copies were found in the National Office.

The primary reasons for the existence of unauthorized software are:

- Multiple platform system configuration contributes to VETS' software management problems;
- Lack of awareness and understanding of policies;
- Employees introduced personal (employee-owned) software; and
- VETS does not account for its software products through an appropriate record-keeping system.

The Director of VETS' Office of Agency Management and Budget has acknowledged the existence of unauthorized software and plans to issue a request to all employees asking for the removal of all unauthorized software applications. In addition, VETS will incorporate a section in its Management Control Review instrument requiring internal review teams to check personal computers to see if they have unauthorized or unlicensed applications.

Further detail is provided below.

Multiple platform system configuration contributes to VETS' software management problems

VETS Nationwide

The use of different platforms across VETS' offices compounds the problems of software management since well defined control points and procedures need to be in place to handle the different platforms.

Although we were informed by both ITC and VETS' managers that they plan to install the WindowsNT platform on VETS computers, we did not obtain an official plan detailing the actual scope and time frames associated with this effort. VETS needs to fully implement the WindowsNT system configuration during the next fiscal year covering the entire VETS organization, or establish procedures to manage software over a multiple platform system configuration.

National Office

Users in the national office cannot install software applications on their desktop computers' "C" drive because the network operating system, WindowsNT platform, security configuration settings do not allow access to the selected computers' hard drive, i.e., users do not have administrative rights to their "C" drive. In fact, we were unable to complete our audit in the national office without assistance from OASAM giving us special access privileges for continuing our audit. Our audit software application needs access to the "C" drive in order to perform the audit successfully. Limiting access to the "C" drive is a good control, and OIG understands that all VETS' regions are in the process of being converted to this system configuration.

However, we found that not all national office computers are configured in this manner. Reviewing a sample of 12 computers, we found 5 computers did not have restricted administrative rights. Those five computers contained three unauthorized software products. Two of the five computers are operating under a Windows95 platform while the other three are WindowsNT with special developer access rights.

Regional and State Offices

Regional and state offices computers use a Windows95 platform to access the ECN. One computer used a Windows98 platform. This stand-alone computer did not have access to the ECN.

Lack of awareness and understanding of policies

When users are unaware of the agency policies, or they simply ignore it, the potential increases for unauthorized software applications on computers. Software applications are freely and readily available through the internet, and anyone with limited knowledge about computer technology can easily download these application onto their computers.

Another reason that can lead to the installation of unauthorized software is when software purchased by the agency is shipped to a regional or state office, it sometimes comes packaged with other bonus, demo, or additional software that bear no functional relationship to the primary authorized software. Since the end user is asked to install the software, there are risks that the user may find the additional software interesting and install it along with the primary software. This is evidenced by our discussion with one State office staff who acknowledged installing a software product, which was "bonus" software, without knowing this was against agency policy.

In a response to the OIG *Statement of Facts*, VETS admitted not having guidance as to authorized software and a process to follow before this calendar year. As a result, their previous procedural guidance did not have the same standards. VETS stated that the administrative guidance will be conveyed to all the VETS' staff.

An example of the effect of not being aware of the policies is apparent with the existence of an application, available from the internet, created by the Webshots Corporation. Users access the company website to obtain thousands of free photos for decorating their monitor screens. There were eight occurrences found of this particular software application. For one, management was unaware of the existence and functionality of this software product. Secondly, the finding of 8 copies of this product on the employees' computers attest to their

lack of knowledge in terms of the agency policy and the potential threats associated with this application.

This application was downloaded on one of OIG's computers for test purposes. After removing the application, we noticed problems with our system. For example, launching the web browser automatically opened the Webshots company website as opposed to the normal OIG homepage. Further, the operating system internet options settings were disabled preventing the user to reset the normal default. The problem required the intervention of OIG's computer assistance division to fix the problem.

The Department's DLMS 9, Chapter 1200 policy states that Department of Labor employees are prohibited from loading undelivered or personal software unless specifically authorized by the agency. As such, VETS needs to ensure computer users are adequately informed about the use of unauthorized software as a way of reinforcing its controls over this issue.

Employees introduced personal (employee-owned) software

OIG identified two unauthorized software applications (CareerPath 98 and Organization Chart 2.0) that had been purchased personally by VETS' employees. VETS officials stated these particular tools, although unauthorized, were used for mission-related activities.

The use of personal (employee-owned) software to conduct government business introduces the potential for the following unnecessary risks:

- Government files, data, and applications can be negatively impacted.
- Difficulties in maintaining transferable technology and compatibility with existing IT environments.
- Lack of appropriate purchasing and licensing documentation following prescribed government rules and regulations.
- Inappropriate or no vendor support.

The Department's DLMS 9, Chapter 1200 policy states that Department of Labor employees are prohibited from loading undelivered or personal software unless specifically authorized by the agency.

The Director of VETS' Office of Agency Management and Budget plans to take action by issuing guidance to all its employees. This guidance will state that employees are not to install privately acquired software on their computers, regardless of the software's intended use or the method by which it was acquired. A request from the Director's office was also e-mailed to the responsible regions asking for immediate removal of the privately owned software applications.

VETS does not account for its software products through an appropriate record- keeping system

VETS does not have a software inventory and record-keeping system that contains pertinent information such as publisher name, number of licenses owned / purchased, geographical location of installed software applications, etc.

When OIG requested a list of authorized software from VETS in an attempt to create a software profile, OIG was referred to OASAM for this information. OASAM which operates the ECN network, used by VETS, provided us a network software list. The list also included software acquired by VETS that had been certified by OASAM for use on the ECN. VETS informed us this list was incomplete, and referred us yet to another contact in OASAM for a more complete list. This new list still did not contain the standalone software applications installed in the remote sites.

For example, we were unable to obtain any form of records substantiating the purchase of Lotus 1-2-3 (5.0 and 9.0) software products. While VETS relies on the Department for keeping track of this documentation, a good record-keeping system could have assisted management in recognizing that two versions of this software product existed on its computers. Installing multiple versions of the same software product carries the risks of license violations, maintenance problems, and difficulties in processing data. The Department states that these products were installed long ago and, as a result, they are unable to produce related purchase and licensing documentation.

EO 13103 relating to computer software piracy states that:

> *Each agency shall establish procedures to ensure that the agency has present on its computers and uses only computer software not in violation of applicable copyright laws. These procedures may include:*
>
> *A. preparing agency inventories of the software present on its computers.*
>
> *B. determining what computer software the agency has the authorization to use.*

VETS should consider adopting the procedures designed to keep track of software applications residing on desktop computers it controls. VETS should follow EO 13103 guidance relating to agency software inventories and determination of authorized software.

Although VETS relies on the Department for much of its IT infrastructure, VETS must assume responsibility and accountability for software under its control. A good record-keeping system is especially important for VETS to be aware of which software products reside on the computers it owns.

CONCLUSION

VETS has a multiple platform system configuration which compounds its software management problems. This is evidenced by 35 copies of unauthorized software products found in both the national office and regional and state offices.

We also found that employee-owned software was used in VETS for conducting government business. Actions are being taken by the Director of VETS' Office of Agency Management and Budget for the removal of the employee-owned software from VETS' computers.

RECOMMENDATIONS

We recommend the VETS' Assistant Secretary initiate the following corrective measures to improve the agency's software management:

1. Remove all unauthorized software applications identified by our audit.

2. Fully implement WindowsNT system configuration during the next fiscal year to cover the entire VETS' organization, or assist VETS in developing procedures to manage software over a multiple platform system configuration.

3. Communicate (e.g., *VETS' Alert*) on a regular basis to make VETS' employees aware of the importance of using only authorized software.

4. Work closely with the Chief Information Officer (CIO) and the Office of the Assistant Secretary for Administration and Management's (OASAM) Information Technology Center (ITC) Director for ensuring that explicit software requirements are developed to meet VETS' needs.

5. Assign responsibilities for the purpose of developing a software inventory and a record-keeping system design to identify all software product purchases and related license agreements.

6. Develop and maintain on a continuing basis an updated list of all authorized software used by VETS by performing periodic inventories of software.

ACRONYMS

CAD	Computer Aided Design
CIO	Chief Information Officer
DLMS	Department of Labor Manual Series
DOL	Department of Labor
ECN	Employee Computer Network
EO	Executive Order
GAS	Government Auditing Standards
IT	Information Technology
ITC	Information Technology Center
LAN	Local Area Network
OASAM	Office of the Assistant Secretary for Administration and Management
OIG	Office of Inspector General
PC	Personal Computer
SID	Software Identification Database
VETS	Office of Veterans' Employment & Training Service

GLOSSARY

Copyright:

Form of statutory protection, which allows its owner the exclusive right to control, among other things, the copying, distribution and preparation of derivative works of authored materials. International treaties and laws in most countries provide for protection of software under copyright provisions.

Software license agreement:

Legal agreement between a software user (the licensee) and the software developer that sets the terms and conditions under which the software and its accompanying materials may be used.

Types of licensing agreements:

Stand-alone licenses are commonly used to describe two types of licensing arrangements: a machine license that restricts use to a particular computer, and a single-user license that restricts use to an individual.

Site licenses (also referred to as building licenses) permit the licensee to make as many copies as needed, provided they are used at just one site or building.

District licenses allow the licensee to put multiple copies of the software on personal computers located in offices throughout the organization. In some instances, the licensee must specify the sites or offices where the software will be used.

Network licenses (also referred to as file-server licenses) permit the licensee to install the software on a file server. In some cases, the licensee may restrict the numbers or location of computers on the local area network.

Volume licenses allow the licensee to have a specific number of users within either a office site or an entire organization. This number is often based on average daily attendance.

Operating System:

The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Windows 95/98/Me:

A family of operating systems for personal computers. Windows provides a graphical user interface (GUI), virtual memory management, multitasking, and support for many peripheral devices.

WindowsNT:

The most advanced version of the Windows operating system. Windows NT (New Technology) is a 32-bit operating system that supports preemptive multitasking.

There are actually two versions of Windows NT: Windows NT Server, designed to act as a server in networks, and Windows NT Workstation for stand-alone or client workstations.

ATTACHMENT A

IDENTIFICATION OF UNAUTHORIZED SOFTWARE

PUBLISHER	SOFTWARE NAME	TIMES FOUND
Individual Software Inc.	CareerPath 98	1
Vizacom, Inc.	Animator 4.0	1
" " " "	Media 4.0	1
Intuit	TurboTax Autorun	1
" "	TurboTax 99	1
Liquid Audio, Inc.	Liquid Audio Configuration	1
Village Center, Inc.	Screen Mate Poo 1.0	1
Pervasive Software	Btrieve Utilities for Windows	1
Apple Computer, Inc	MoviePlayer 3.0	2
" " " " " "	Picture Viewer 3.0	2
" " " " " "	QuickTime Info 3.0.2	2
SoftStuff Corp	Wallpaper Changer 2.0	1
America Online, Inc.	AOL 3.0	1
UPS of America	Online Office 6.0.14	1
The Learning Co.	PrintMaster 2.0	2
" " " " "	Cartoon-O-Matic 2.0	2
Comet Systems, Inc.	My Comet Cursor 1	1
MetaCreations Corp.	Kai's Power Goo	1
Sierra On-Line	Internet Gaming 3.0	1
" " " "	Print Artist 4.02	1
BannerBlue Software	Organization Chart 2.0	2
The Webshots Corp.	Desktop Tray 1.3.0	4
" " " " "	Swebexec 1.3.0	4

TOTAL UNAUTHORIZED SOFTWARE COPIES: 35