Office of Inspector General

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

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

FINAL REPORT

Report Number: 23–02–005–10–001
Date Issued: August 19, 2002

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) conducted an audit to determine whether the Occupational Safety and Health Administration (OSHA) has proper procedures in place to ensure authorized computer software products are not used in violation of copyright laws, and whether unauthorized software products exist on the agency's computers.

During our audit, we scanned 166 randomly selected computers in OSHA's National, regional and area offices, and OSHA's Technical Center (laboratory) in Salt Lake City, Utah. We found 221 unauthorized software products, including 27 different computer games. We found no violations of copyright laws for authorized software products.

In addition to the potential software piracy issue, the installation and use of unauthorized software products creates other unnecessary risks for OSHA, such as the possible introduction of computer viruses. The use of unauthorized software can also degrade computer functionality, as the unauthorized products consume memory and processing time.

Inadequate software management policy and procedures contribute to the installation and use of unauthorized software on agency computers. For example, OSHA does not conduct periodic software inventories and, as a result, cannot maintain a complete and accurate listing of unauthorized software.

To improve agency software management and prevent the installation of unauthorized software products, we recommend that the Assistant Secretary for Occupational Safety and Health:

1. Remove all unauthorized software applications and games identified by our audit, including older version, software products. Legally purchased older software products should be removed from individual workstations and stored in a safe location.

2. Develop and perform a periodic (at least once per year) software inventory and use this inventory to maintain an updated list of all OSHA authorized software.

3. Revise and update OSHA Directive PRO 3.5 dated June 9, 1993, to include current hardware and software standards and establish procedures on the monitoring of information technology (IT) assets including a review of IT Acquisition forms and license agreements.

---- ---- ----

Based on OSHA's response to the draft report, and the planned corrective actions, the OIG has resolved all of the above recommendations. OSHA agreed to take steps for the purpose of addressing and resolving OIG's recommendations (Appendix A). However,

OSHA has taken exception to the Webshots purchase example used by OIG in the draft report. OSHA does not discourage the use of screen savers, and OSHA believes the discussion of the Webshots purchase was unnecessary since it went beyond the stated scope of the audit. While the OIG acknowledges OSHA's request to delete the discussion of the Webshots purchase, the OIG does not view the information as extraneous to the audit report.

BACKGROUND

Software piracy occurs whenever a software program is downloaded and 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. Federal copyright statutes protect the license agreements. 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 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. EO 13103 encourages government agencies to prepare software inventories and determine which software products they are authorized to use.

The OSHA nationwide network, the OSHANET, provides employees with IT resources to help them effectively perform their OSHA duties and responsibilities. The OSHANET encompasses user workstations, servers, network devices, software, and data communications equipment. OSHA's Directorate of Information Technology is responsible for the management and administration of the OSHANET.

OBJECTIVES, SCOPE, METHODOLOGY AND CRITERIA

OBJECTIVES

The objectives were to determine whether OSHA has the proper controls and procedures in place to 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 OSHA's National Office and Technical Center in Salt Lake City, Utah, and selected regional and area offices.

We scanned a total of 166 workstations, which included 104 in the National Office and 62 in OSHA regional and area offices in Chicago, Dallas, Philadelphia, San Francisco, and OSHA's Technical Center in Utah. Computers in the National Office, regional offices, area offices, and the Technical Center were selected for testing based on a random sample.

The audit was conducted during the period of May 30, 2001 through March 15, 2002. An exit conference was held on March 18, 2002.

METHODOLOGY

The audit was conducted in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States.

OIG used a software tool developed by Attest System, Inc., titled Gottlieb & Associates Search Program (GASP 5.2) to test OSHA's computers. Using this tool, OIG performed a scan of 166 workstations in OSHA to detect whether unauthorized software was installed on the computers. Specifically, we scanned a total of 104 workstations in the National Office and 62 workstations throughout various regional and area offices to determine whether any appeared unusual or suspect. The audit software was 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 programmed 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. Upon completion of the scanning process, analyses were performed to identify unauthorized software products.

We requested a list of authorized software and supporting documentation from OSHA in an attempt to create a software profile. OSHA's list of 18 software titles, however, was not detailed or comprehensive enough to allow scanning using the GASP profiling feature. As a result, we were not able to generate exception reports for software products not matching the profiled information. Our procedure, instead, consisted of scanning individual workstation computer "C" drives to capture all software products contained in

each individual workstation computer. This resulted in extending the audit's period of performance.

A list of software products found to be unusual by OIG was submitted to OSHA for its review and determination as to whether the software was authorized for use in the agency and whether accompanying documentation (i.e., license agreements, purchase orders, requisitions, and approval forms) existed. OSHA's review resulted in its providing us with additional documentation that increased the original list of authorized software products from 18 to 145, an increase of 127 products.

The additional 127 software products, with the accompanying documentation, were reviewed by OIG to determine whether the additional software products corresponded to OIG's list of software identified as unusual (Exhibit A).

In establishing audit results, a distinction is made between copies of software and number of software packages. The number of copies found for the games in OSHA is the total occurrences of games found, i.e. the same game may be counted more than once as it appears on more than one computer. The number of software packages only counts a particular application once (per geographical location) regardless of how many times it was found on different computers (Exhibit B). OIG does have the information available should OSHA need to know specifically how many copies were found for each software application. However, for the purpose of presenting the results in Exhibit B, OIG does not show the number of copies found.

In addition to scanning, our assessment was limited to policies and procedures covering internal controls relative to copyright/licensing requirements and software authorized for use on individual workstations.

CRITERIA

We used as criteria for this audit the U.S.C. Title 17, Chapter 5, Copyright Law Infringement and Remedies; Executive Order (EO) 13103, Computer Software Piracy; the Department of Labor Manual Series (DLMS-9) Chapter 1200, Microcomputer and LAN Management; OSHA Directive (PRO 3.5) – End-User Computer (EUC) Policy; and OSHA Directive (ADM 1-0.19) OSHANET Acceptable Usage Policy.

U.S.C., Title 17, section 504 (as limited by 28 U.S.C. 1498 (b)) states that a civil action may be instituted against the Federal Government for actual damages.

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.

OSHA Directive PRO 3.5 establishes policy, guidelines, standards and procedures, and assigns roles and responsibilities for the acquisition of End-User Computer (EUC)

resources including stand-alone workstations, laptop computers, and associated software and peripherals for amounts not exceeding $2,500.

OSHA Directive ADM 1-0.19 OSHANET, Acceptable Usage Policy, describes and sets forth guidelines for use of OSHANET and any of its resources. Software products not properly licensed and authorized for use by OSHA should not be installed or run on any OSHANET workstation or server according to OSHA policy.

FINDINGS AND RECOMMENDATIONS

OIG found that unauthorized software products and copies of games reside on OSHA's computers, and that OSHA needs to strengthen controls over software management policies and procedures.

I. UNAUTHORIZED SOFTWARE EXISTS IN OSHA

During our audit, we scanned 104 workstations in the National Office and 62 workstations in various regional and area offices, and OSHA's Technical Center in Salt Lake City, Utah. Our analysis of the results of these computer scans identified the following unauthorized software products:

Applications

- 194 software applications were determined to be unauthorized based on the information provided by OSHA (Exhibit A) after review of 203 questionable software applications (Exhibit B);

Games

- 136 copies of 19 different Microsoft Corporation software games were found on workstations; and

- 30 copies of 8 different software games by various software publishers other than Microsoft Corporation were found on workstations.

OSHA DIT stated that, in accordance with OSHA's policy, games should not be installed on workstations. OSHA stated that games were allowed in the past for users to practice mouse and cursor movement, but remarked that OSHA has not gone back to disable the operating system option that gives the users access to this function.

OSHA Directive, ADM 1-0.19 – OSHANET Acceptable Usage Policy, Chapter X – paragraph B, items 4 and 11 state that playing games and loading unauthorized or personal software is considered non-acceptable personal use.

The use of unauthorized software creates unnecessary risks for the agency. In addition to the potential software piracy issue, the use of unauthorized software can lead to the

introduction of viruses, and degradation of computer functionality, as memory and computer processing are allocated to users of unauthorized software.

II. INEFFECTIVE SOFTWARE MANAGEMENT POLICIES AND PROCEDURES

OIG found key areas that can improve OSHA's ability to manage agency software. These areas include taking a periodic software inventory, establishing an effective mechanism for the certification and authorization of software, and monitoring and replacing versions of software products as software updates are introduced.

A. OSHA Needs to Prepare an Authorized Software Inventory List and Keep It Current

The OIG identified 203 questionable software products on OSHA's computers as a result of scanning. OIG then requested confirmation from OSHA on the legitimacy of the 203 specific questionable (potentially unauthorized) software applications.

Since OSHA does not have a software inventory, OSHA was not able to directly address OIG's list of 203 software applications. Instead, OSHA chose to use supporting documentation from all previously authorized software covering its National, regional and area offices, and provided this information to OIG. OIG used this information in its analysis of OSHA approved software in lieu of an agency software inventory.

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.

In addition, OSHA's own EUC policy (PRO 3.5) states "Federal regulations and Departmental policy require OSHA to maintain an accurate inventory of all information technology acquisitions." It states that those acquisitions "include freeware and shareware" and that the Office of Management Data Systems (OMDS) is responsible for maintaining OSHA's information technology inventory.

By not having a complete, up-to-date inventory, OSHA does not know what is installed on its computers and is unable to ensure computer software products are used in accordance with software copyright laws, licenses, and agency standards.

B. Ineffective Controls Over Certification/Authorization Checklist Form

During the audit, OSHA provided documentation supporting legal ownership of its software products. OIG noticed that the forms used to authorize and certify the acquisition of EUC resources not exceeding $2,500 were not always signed, and lacked appropriate information for the purpose of justifying related acquisitions.

1. Forms not always signed

OSHA uses a Certification/Authorization Checklist Form that is used to identify the need and justification for acquiring software. The use of this form appears to be inconsistent and not serving the purpose intended by OSHA's policy.

The form is to be approved by the appropriate Directorate Head in the National Office, and should be approved by the Regional Administrators for area, district, and regional offices. OIG observed, however, the forms are not always signed. For example, all signature lines are left blank on some forms, and only the area office official signed others.

OSHA's policy (PRO 3.5 – End-User Computer –EUC Policy) states that:

> EUC requests are to be submitted by Area, District, and Regional Office managers to the appropriate Regional Administrator for review, approval and processing.

An unsigned Certification/Authorization form indicates that a request for a particular software application has not been properly authorized, and that OSHA is not implementing internal controls consistently.

2. Insufficient justification

The Certification/Authorization Checklist Form does not clearly justify software application needs. The "Justification" section of the form is a blank that is to be filled in by a one word description of the reason why the software is necessary and required. In one case, OIG observed that one software application authorized through the use of this form was Webshots by The Webshots Corporation. The justification for this software being required to benefit the agency is that it is necessary to "perform screensavers." Webshots allows individuals to customize screensavers, wallpaper and electronic postcards, as well as download photos in Webshots photo albums. The purchase of screensavers would not be required as this function is available through the Windows desktop properties.

OIG also found there are potential threats associated with applications such as Webshots. Webshots 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.

OSHA's policy (PRO 3.5 – End-User Computer –EUC Policy) establishes identification of needs and justification criteria by stating that:

> Decisions to acquire new EUC resources (smaller than $2,500) shall be based upon individual, workgroup and program needs, established priorities and existing resources. Furthermore, needs shall be presented in the form of a written justification that is based on increased efficiency, improved effectiveness, or innovation. The same criteria are followed for freeware and shareware.

Without having sufficient information to make a decision on whether to approve a particular application, the approving official may be certifying software that is not necessary for the benefit of the agency. For example, the one word description used for stating the reason for acquiring Webshots was not enough for OSHA to properly assess the necessity of this application. The approving official would need more details on the functionality, features, utility, and nature of this software.

C. OSHA Does Not Monitor Outdated Software Product Versions

The original list of authorized software applications given to OIG auditors was composed of version specific applications. However, our audit showed that some software applications installed on OSHA's computers included various versions of the same application. The following example illustrates this point:

- OIG found 5 copies of WordPerfect for DOS 5.1 on 4 computers in the National Office, i.e., one computer had 2 copies of WordPerfect for DOS 5.1.

- OSHA's original authorized list of software application included WordPerfect 8.0 as the authorized version. We expected we would find WordPerfect 8.0 to be the standard word processing software installed on OSHA computers. However, we found WordPerfect versions DOS 5.1, 6.1c, 7.0.1a, and 8.0.

OSHA's Directive (PRO 3.5) includes a section on Compatibility and Connectivity Standards and Guidelines. In this section, it is stated ". . . to bring OSHA into compliance with Federal regulations and the Department 'ITA-2000' initiative, the Agency has established three basic categories of EUC resources."

"OSHA Standard EUC Resources" outlines what software products are authorized for use in OSHA. OSHA's standard software includes a list of version specific software products, such as WordPerfect 5.1, and Lotus 1-2-3 Version 3.1. OIG observed that OSHA's computers contained multiple versions of various software products (as identified on Exhibit B). OSHA does not appear to be following its own policy. This

directive and standards contained within, however, are old and outdated, i.e., OSHA Directive PRO 3.5 is dated June 9, 1993.

Uniformity and software version control are important when implementing standards in order for users to be able to seamlessly exchange data. For example, OSHA maintains WordPerfect DOS 5.1 but the agency's standard is WordPerfect 8.0. Also, some software products that are available as shareware, for instance, specifically state that the publisher does not have an obligation to support previous (older) versions of its products. For example, the Acrobat Reader's licensing agreement states the following:

> If the Software is an Update to a previous version . . . you may continue to use the previous version of the Software on your computer after you receive the Update to assist you in the transition to the Update, provided that . . . you acknowledge that any obligation Adobe may have to support the previous version of the Software may be ended upon availability of the Update.

OSHA has expressed concern over the need to remove older software applications. OSHA believes its decision to support the older applications is acceptable since the agency legally purchased the software.

If OSHA legally purchased software, which is currently outdated and not part of the standards, it would be best to remove the software from individual workstations and store the program disk(s) in a safe location. The applications can be accessed and installed temporarily should OSHA have a need for this application that cannot be met by newer authorized standard versions. In addition, having everyone using the latest version of a software product prevents potential problems associated with technical support of outdated versions.

CONCLUSION

Our audit found that unauthorized software products exist in OSHA and ineffective software management policies and procedures that need to be revised to include new hardware and software standards as well as proper inventory procedures.

OSHA will benefit from strengthening its software management controls by ensuring the prevention of unauthorized software use and potential software piracy. OSHA has recognized this benefit by stating it is committed to follow OIG recommendations in order to improve software management.

RECOMMENDATIONS

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

1. Remove all unauthorized software applications and games identified by our audit, including older version, software products. Legally purchased older software products should be removed from individual workstations and stored in a safe location.

2. Develop and perform a periodic (at least once per year) software inventory and use this inventory to maintain an updated list of all OSHA authorized software.

3. Revise and update OSHA Directive PRO 3.5 dated June 9, 1993, to include current hardware and software standards and establish procedures on the monitoring of IT assets including a review of IT Acquisition forms and license agreements.

Management Comments

OSHA's Assistant Secretary provided comments in reference to the above recommendations on July 15, 2002. OSHA has taken exception to the Webshots purchase example used by OIG in the draft report. OSHA does not discourage the use of screen savers, and OSHA believes the discussion of the Webshots purchase was unnecessary since it went beyond the stated scope of the audit. While the OIG acknowledges OSHA's request to delete the discussion of the Webshots purchase, the OIG does not view the information as extraneous to the audit report. OSHA's comments have been included as part of this report in Appendix A.

OIG Response

Although OSHA disagrees with OIG about the issues concerning older version software products and screensavers, the OIG has resolved all of the above recommendations based upon OSHA's planned corrective actions, and will continue to work closely with OSHA to bring each to closure.

ACRONYMS

ADM	Administrative Directive
CIO	Chief Information Officer
DIT	Directorate of Information Technology
DLMS	Department of Labor Manual Series
DOL	U. S. Department of Labor
DOS	Disk Operating System
EO	Executive Order
EUC	End User Computer
GAS	Government Auditing Standards
GASP	Gottlieb & Associates Search Program
IT	Information Technology
ITA-2000	Information Technology Architecture - 2000
LAN	Local Area Network
OIG	Office of Inspector General
OMDS	Office of Management Data Systems
OSHA	Occupational Safety and Health Administration
OSHANET	Occupational Safety and Health Administration Network
PRO	Procedure Directive
SID	Software Identification Database
U.S.C.	United States Code

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 an office site or an entire organization. This number is often based on average daily attendance.

U.S. Department of Labor

Assistant Secretary for
Occupational Safety and Health
Washington, D.C. 20210

JUL 15 2002

MEMORANDUM FOR: ELLIOT P. LEWIS
Deputy Inspector General for Audit

FROM: JOHN L. HENSHAW

SUBJECT: OSHA's Responses to Strengthening OSHA's Software Management Controls Can Prevent Unauthorized Software Use and Potential Software Piracy
Draft Report No. 23-02-005-10-001

This memorandum transmits OSHA's response to your June 28, 2002 request for written comments addressing the OIG's findings and recommendation.

If you have any questions regarding our comments, please contact Cheryle A. Greenaugh, Director of the Directorate of Information Technology at (202) 693-1818.

Attachment

ATTACHMENT - OSHA's Responses to Strengthening OSHA's Software Management Controls Can Prevent Unauthorized Software Use and Potential Software Piracy, Draft Report No. 23-02-005-10-001

BACKGROUND

The OIG scanned 166 randomly selected computers in OSHA's national, regional and area offices, and OSHA Salt Lake City Technical Laboratory. They found 221 unauthorized software products, including 27 different computer games.

FINDINGS:

I. Unauthorized Software Exists in OSHA

A. Applications – 194 applications were determined to be unauthorized based on the information provided by OSHA after review of 203 software questionable applications

OSHA Management Response: In response to the OIG audit, OSHA conducted an extensive nationwide paper review of all software currently installed on the desktops in January 2002 in all offices, not just those surveyed by the OIG. As a result of this manual audit, software was removed from desktops that were not authorized. OSHA's Directorate of Information Technology provided the OIG with a list of the authorized software and the paperwork associated with the enhanced list of authorized software on February 8, 2002. All software was purchased for use of the staff in the office to perform their work.

B. Games – 136 copies of 19 different Microsoft Corporation software games were found on workstations. 30 copies of 8 different software games by various publishers other than Microsoft Corporation were found on the workstations.

OSHA Management Response: All games have been removed from OSHA desktops and OSHA staff have been instructed again that games are not to be installed on their desktops.

II. Ineffective Software Management Policies and Procedures

A. OSHA needs to prepare an authorized software inventory list and keep it current

OSHA Management Response: OSHA concurs with this finding and will prepare and maintain an authorized software inventory list.

B. Ineffective Controls Over Certification/Authorization Checklist Form

OSHA Management Response: OSHA acknowledges the concerns raised by the OIG audit and the need to update Directive PRO 3.5 dated June 9, 1993. OSHA uses the IT Acquisition Certification form to request software and hardware. The OIG identified that the Regional Administrators should have signed off on the form in the area, district and regional offices and the appropriate Directorate Head in the national office. OSHA will review this process and revise the Directive if necessary. OSHA's Information Technology Executive Steering Committee has also made changes to the acquisition of hardware and software. In the first quarter of FY 2003, OSHA's Directorate of Information Technology will convene a small workgroup that will revise and reissue this Directive.

OSHA takes exception to the Webshot purchase example used by the OIG in this section of the Draft report. While we agree that the section on justification could have been more descriptive, it was sufficient to determine its purpose since OSHA does not discourage the use of screen savers for personalization purposes. By contrast, OSHA believes that the subsequent discussion of the Webshot purchase was unnecessary since it went beyond the stated scope of the audit. We do not believe that the fact that this software caused problems on the OIG's computer is reason to document it in this report on the use of authorized software. For the record, OSHA will incorporate the use of screen savers in its revised Directive PRO 3.5. However, the agency requests that the discussion of the Webshot purchase be deleted as extraneous to the audit report.

C. OSHA does not monitor outdated software product versions

OSHA's Management Response: OSHA owns the licenses to older versions of WordPerfect 5.X up to the 8.0 versions cited. The older versions of the software were found in the old archived files on the desktops. The software is not illegal to use so reference to it in an audit whose purpose was to document illegal software seems to be misplaced. The standard software that OSHA currently uses is WordPerfect 8. The agency will be able to monitor older versions of the software when it puts procedures and policies in place for software inventory. OSHA does not see this as an issue.

RECOMMENDATIONS:

1. Remove all unauthorized software applications and games identified by our audit, including older version, software products. Legally purchased older software products should be removed from individual workstations and stored in a safe place.

OSHA's Management Response: OSHA has removed all unauthorized applications and games that we have not purchased. Removing legally purchased software was not the focus of this audit nor does the agency necessarily agree with the OIG's position on this. The agency will commit to sending periodic friendly reminders to OSHA staff beginning in July 2002 with regard to proper policies and procedures with respect to software.

2. Develop and perform a periodic (at least once per year) software inventory and use this inventory to maintain an updated list of all OSHA authorized software

OSHA Management Response: OSHA will begin a periodic software audit and use this inventory to maintain an updated list of authorized software beginning January 2003. OSHA will prepare a training session available via the Intranet on "How to Complete an IT Acquisition Certification Form" by September 30, 2002.

3. Revise and update OSHA Directive PRO 3.5 dated June 9, 1993, to include current hardware and software standards and establish procedures on the monitoring of information technology (IT) assets including a review of IT Acquisitions forms and license agreements.

OSHA Management Response: OSHA will revise Directive PRO 3.5 for distribution in January 2003