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