ADMINISTRATIVE COMMUNICATIONS SYSTEM

UNITED STATES DEPARTMENT OF EDUCATION

Office of Management, Executive Office

400 Maryland Avenue; Washington, DC 20202

Transmittal Sheet #:	2004-0014	*Date:*	September 30, 2004
Distribution:	All ED employees	*Distribution Approved:* *Directives Management Officer:*	/s/ Tammy Taylor

Action: Pen and Ink Changes

Title: Handbook for Software Management and Acquisition Policy

Number: Handbook OCIO-08

Document Changing: Handbook OCIO-08, *Handbook for Software Management and Acquisition Policy*, dated 08/25/2003.

Summary: To effectively meet compliance standards, applicable laws, and licensing restrictions as outlined by Executive Order 13103, on Computer Software Piracy, the Department is implementing this Software Management and Acquisition Policy. This SMA Policy will set forth steps the Department will take to comply with the Order and Implementing Guidelines issued by the Chief Information Officers Council and managed by the OCIO.

Pen and Ink Changes: The following pen and ink changes have been made to reflect OCIO's reorganization and the renaming of OCFO/CPO to OCFO/CAM.

Page	*Section*	*Changed*	*To*
1-15	Date	08/25/2003	09/30/2004
1	Superseding Information	Information described above	Information described above
1	Technical Contact Phone Number	For technical questions regarding this ACS document, please contact Wanda Davis via e-mail or on 202-708-5796.	For technical questions regarding this ACS document, please contact Wanda Davis via e-mail or on 202-245-6444.
5	V. B.	Office of the Chief Information Officer (OCIO)/IT	Office of the Chief Information Officer (OCIO)/IAMT (Investment and Acquisition Management Team)
5	V. E.	Contracts and Purchasing Operations (CPO)	Contracts and Acquisitions Management (CAM)
11	VI. Q. 1st paragraph, 2nd and 3rd sentences	CPO	CAM

ADMINISTRATIVE
COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL HANDBOOK

Distribution:
All Department of Education employees

Approved by: _____/s/_____(08/25/3003)__
William J. Leidinger
Assistant Secretary
Office of Management

Handbook for

Software Management and Acquisition

Policy

Supersedes ACS Handbook OCIO-08 "Handbook for Software Management and Acquisition Policy" dated 08/25/2003.

For technical questions regarding this ACS document, please contact Wanda Davis via e-mail or on 202-245-6444.

Table of Contents

I. Purpose

To effectively meet compliance standards, applicable laws, and licensing restrictions as outlined by Executive Order 13103, on Computer Software Piracy, the U.S. Department of Education (Department) is implementing this Software Management and Acquisition Policy (SMA Policy). This SMA Policy will set forth steps the Department will take to comply with the Order and Implementing Guidelines issued by the Chief Information Officers Council (CIOC) and managed by the Office of the Chief Information Officer (OCIO).

II. Policy

The Department will work diligently to prevent and combat computer software piracy as well as ensure all software installations are properly licensed. Specifically, the Department will ensure that it does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.

III. Authorization

Executive Order 13103, titled Computer Software Piracy signed by President Clinton on September 30, 1998 (see Attachment A.) The Order can be found at 63.Fed.Reg.53273 (October 5, 1998).

IV. Applicability

This Directive applies to all Department employees, and all contractors utilizing the Department's owned information technology equipment and software. This Directive applies to all Information Technology (IT) equipment connected or not connected to the Department's Educational Network (EDNet).

The Department's IT Security Program Management Plan (ITSPMP) under Section 2.1 Governance paragraph two states "For each system and application within the Principal Offices, the Computer Security Officers (CSO) and System Security Officers (SSO) will assist in and monitor the implementation and effectiveness of the Department's IT security governance program."

The Secretary has formally endorsed the security goals outlined within the ITSPMP and is responsible for the implementation of the Department's IT Security Program in accordance with the Federal Information Security Management Act (FISMA).

Executive Order 13103 Section 2 (a) states: "ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency's computers."

V. Responsibilities

OCIO is responsible for establishing the Department procedures in the area of software licensing management. OCIO manages and monitors all Department-approved standard licensed software media. In support of this SMA Policy, roles and responsibilities have been identified for:

A. Chief Information Officers Council (CIOC)

Principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software.

B. Office of the Chief Information Officer (OCIO)/Investment and Acquisition Management Team (IAMT)

Ensures agency compliance with copyright laws protecting computer software and ensures only authorized computer software is acquired for and used on the agency's computers. Additionally, OCIO maintains a Software Library for approved software media, along with a current and updated license-tracking system.

C. CIO Customer Connection (CCC) Help Desk

Creates a HEAT ticket for all software installation throughout the Department. HEAT is the call tracking system OCIO uses to provide technical support.

D. Computer Security Officer (CSO)

Formally designated by the business or functional managers to be responsible for the implementation of the Department's IT security program within their organization.

E. Contracts and Acquisitions Management (CAM)

Located with the Office of the Chief Financial Officer (OCFO), responsible for establishing policy for, the solicitation, award, administration, and closeout of all contracts, simplified acquisitions, and orders under government wide contract vehicles (e.g. GSA Schedules, GWACS). Responsible for delegating Contracting Officer authority to agency procurement officials.

F. Contracting Officer (CO)

Department employees that have written specific delegated procurement authority to purchase goods or services. Must comply with the provisions of this directive if authorized to purchase software. Ensures performance of all necessary actions for effective contracting. Ensures compliance with the terms of the contract and safeguards the interests of the United States in the contractual relationship.

G. Contracting Officer Representative (COR)

Designated program official for technical monitoring of individually designated specific contracts; ensures compliance with the technical requirements of the contract or order.

VI. Procedures and Requirements

A. Software Acquisition and Installation Procedures

OCIO implemented the following procedures to avoid acquisition of illegal software. Please review the Product Support Plan (PSP) located at: http://connected.ed.gov/index.cfm?navid=226 (Connected, IT & Management, EDNet/Network) which is designed to communicate the supported EDNet products.

1. Requisitions for software and upgrades will be submitted to OCIO by the Contracts and Purchasing Support System (CPSS) for approval and, upon award, delivery and receipt by the CO, registered in the Software Library.

2. Requests for installation of software or upgrades must be submitted via CCC Help Desk.

3. Software compliance on Section 508 of the Rehabilitation Act is addressed in the Departmental Directive "Procuring Electronic and Information Technology (EIT) in Conformance with Section 508 of the Rehabilitation Act of 1973, as amended". Please review the ACS document The Electronic and Information Technology (EIT) Procurement Procedure (located at Connected, Offices and Groups, Offices on Connected, Office of Management, Executive Office, ACS Directives, Alphabetical listing) to meet all justifications.

4. Acquisitions of hardware, which include bundled software, will be documented and reported to OCIO. OCIO will verify that the Department has an appropriate license for the use of the bundled software.

B. Destruction of Unauthorized Software

OCIO will inform the Principal Office CSO of copies of software for which the Department lacks the appropriate license. The CCC will remove any unlicensed software.

If an application is needed department-wide, OCIO may present a business justification and requirements document for such software. If an application is needed for a specific office, the Principal Office(s) may present a business justification and requirements document to OCIO for review/approval. OCIO will obtain on behalf of the Principal Office(s) software license(s) that meet the guidelines set forth in Executive Order 13103.

C. Software Management Review and Inventory

OCIO will conduct an annual assessment of its software management procedures and practices, and an inventory of installed software and related license agreements, purchase invoices, and other documentation showing evidence of licensed software that is currently in use. OCIO will use automated tools to query Department computers and retrieve reports to assist with enforcing and validating this SMA Policy.

D. Software Library

OCIO maintains a Software Library for original software licenses, certificates of authenticity, purchase invoices, completed registration cards, original software media (e.g., diskettes or CD-ROMs), user information, and assessment information. OCIO will maintain this information in a secure location. .

All software is available to the Department's employees for use (e.g., installation/re-installation, replacement, and upgrades) with approval from OCIO Software Licensing Manager or designee (providing licenses are available) via sign-in and sign-out process. The software is the sole responsibility of the CCC Helpdesk Technician while in their care.

E. Software Use

The following software policy applies to all Department employees and contractors who work at the Department's site.

Prohibition Against Unlicensed Software Use.

No employee or contractor will:

- Install, reproduce, distribute, transmit, or otherwise use software for which the Department lacks the appropriate license, unless such software is properly licensed to the employee or contractor and used in accordance with Department policy and the applicable license. If an employee or contractor becomes aware of the reproduction, distribution, or use of unauthorized software in this Department, the employee will promptly notify his or her supervisor, and the contractor will notify their COR.

- Install, reproduce, or use any software upgrade on a computer that does not already have resident the original, licensed version of the software.

- Loan, distribute, or transmit Department software to any third party, unless the employee or contractor is expressly authorized to do so by OCIO and the applicable license.

F. Authorization to Use Department Licensed Owned Computers Offsite

Authorization to use licensed software on Department-owned computers off-site: (e.g., flexi-place and tele-centers).

Prohibition Against Unlicensed Software Use.

No employee or contractor will download unlicensed or untested software from the Internet or other sources on Department computers unless otherwise directed to do so by OCIO.

G. Enforcement

OCIO will conduct annual reviews and assessments to evaluate the effectiveness of this SMA Policy using automated software tools (i.e., Altiris).

Any software identified in which OCIO does not have a license will be reported to the Principal Office (PO) and CSO, and removed by CCC Helpdesk as outlined in item Q. "Steps to take if Pirated Software is Suspected ".

H. Responsibility

Employee/Contractor Responsibility – It is the employee and contractor's responsibility to ensure that no unlicensed software is installed on the computer.

CSO Responsibility – It is the CSO's responsibility to report to the employee's supervisor the use of unlicensed software, and follow-up with the CCC Help Desk for software removal and the contractor will notify their COR.

Supervisor Responsibility – It is the employee and contractor's supervisors and the COR's responsibility to ensure that unlicensed software is removed from the employee and contractor's desktops once reported by the CSO.

I. Education and Training

The Department will provide training to existing and new employees on compliance with the Executive Order 13103 and this SMA Policy. As part of such education and training, the Department will:

1. Provide training during employee orientation on this SMA Policy on how to detect and prevent piracy, and the consequences of violating this SMA Policy and applicable copyright laws.

2. Circulate reminders of this SMA Policy on a bi-annual basis.

3. Review annually in the Department's Security Awareness Program.

J. Performance Measures

OCIO will develop performance measures to monitor the Department's compliance with the Executive Order 13103, CIOC, and this SMA Policy on a quarterly basis.

OCIO will run quarterly reports on software applications to ensure the Department is in compliance with this directive and policy.

K. Types of Pirated Software

To comply with Executive Order 13103, applicable laws, and licensing restrictions, the Department and its employees should be cognizant of the different types of pirated software when evaluating bids or engaging in negotiations to acquire computer software.

For purposes of this policy, pirated software includes both illegally copied software and software that violates licensing restrictions.

L. Illegally Copied Software

Illegally copied software may include or be generated from: bundle software, compilation CDs, counterfeit software, hard-disk loaded software, online pirated software, pirated software, other illegally copied software.

M. License Misuse

OCIO will review licenses to ensure that the Department's use of the software will not violate any restrictions imposed by the publisher. Examples of misuse include:

1. *Original Equipment Manufacturer (OEM) Software*—OEM software is licensed and specifically marked for distribution with new computer hardware. License misuse occurs when OEM software is "unbundled" from the computer and distributed to, and used by, the end user as a standalone product, often at a heavily discounted price.

2. *Academic Software*—Academic software is manufactured, licensed, and specifically marked for distribution to educational institutions and students at reduced prices. License misuse occurs when academic software is distributed to, and used by, a non-academic end user.

3. *Not for Resale (NFR) Software*—NFR software is marked "not for resale" and typically is distributed as a promotional or a sample product and not licensed for commercial distribution and use. License misuse occurs when NFR software is distributed in violation of its resale restrictions.

4. *Fulfillment Software*—Fulfillment software is licensed solely for distribution to mid- or large-sized end users who currently possess a volume license agreement or valid site license. Fulfillment software is typically distributed in a CD jewel case without the packaging or materials that accompany retail products. The fulfillment media is not a licensed product. License misuse occurs when fulfillment software is distributed to, and used by, end users who lack the necessary licenses for use of the product.

5. *Software Upgrades*—Upgraded versions of software programs are licensed and specifically marked for distribution to users who currently possess a valid license for the original product. License misuse occurs

when upgrades are distributed to, and used by, users who lack a license for the original product.

6. *OEM, Fulfillment, and Other Non-Retail Products*—Typically, OEM, fulfillment, and other non-retail products are distributed without the colorful packaging and materials that accompany full retail products. Accordingly, these non-retail products are easier to counterfeit. Department employees should be aware that deeply discounted non-retail software might in fact be counterfeit.

N. Operational Defects of Pirated Software

The Department and its employees should be aware that the acquisition and use of software in violation of applicable copyrights or licensing restrictions could jeopardize the effectiveness and integrity of the Department's entire EDNet. Pirated software typically lacks the full package of benefits that accompany legitimate products, including the following:

1. Warranty protection

2. Notice of, and ability to obtain, upgrades to the software

3. Technical support for the software

4. Assurance that the software is free of computer viruses

5. Confidence that the most recent defect-free version of the software, is being obtained

O. Avoid Acquisition of Pirated Computer Software

OCIO will take measures to ensure reasonable use of only authorized software. This includes the following:

1. Educate OCIO and Principal Office employees and contractors, who are authorized to request the purchase of software, on the requirements of the Executive Order 13101and this SMA Policy.

2. Before purchasing software verify that the license authorizes distribution to and use by the Department.

3. Purchase software from reputable resellers. OCIO maintains a list of reputable vendors.

P. Warning Signs of Pirated Software

Principal Offices should be aware of the following “warning signs” that often accompany pirated software:

1. The price of the software is significantly below the software publisher's suggested retail price or otherwise appears “too good to be true.”

2. The software is distributed in a CD jewel case without the packaging and materials that typically accompany a legitimate product.

3. The software lacks the software publisher's standard security features, such as a hardware lock or certificates of authenticity.

4. The software lacks an original license or other information from which the Department can verify that the copyright holder validly licenses Department use of such software.

5. The packaging or materials that accompany the software have been copied or are of inferior print quality.

6. The CD contains software from several software publishers or programs that are not typically sold as a "suite."

7. The software is downloaded via the Internet without the software publisher's authorization.

8. The software is distributed via a mail order or on-line reseller who fails to provide appropriate guarantees of a legitimate product.

9. The software contains markings indicating that distribution to, and use by, the Department, would violate the software publisher's license (e.g., "distribute only with new PC hardware," "Academic Version," or "Upgrade").

10. The software is loaded onto computer hardware without a separate license or invoice indicating a legitimate purchase.

Q. Steps to take if Pirated Software is suspected

If an employee or contractor suspects that software offered or supplied by a reseller is pirated, the employee should contact their (PO) CSO and the contractor should contact their CO. If a contractor or vendor has supplied pirated software, CAM should be notified immediately. CAM and the CO, in conjunction with Office of the General Counsel (OGC), Office of the Inspector General (OIG), and the affected offices may choose to take immediate action as deemed appropriate, or take all or any of the following corrective actions:

1. Return the pirated software and request legitimate replacement software or a refund.

2. Withhold payment under the software contract until legitimate software is supplied.

3. Terminate the contract for failure to comply with its terms.

4. Suspend and/or debar the reseller for committing an offense that indicates a lack of business integrity, for engagement in fraud, or for willfully failing to comply with contract terms (debarment only). (See *Federal Acquisition Regulation Subpart 9.4*).

5. Bring a False Claims Act action against the contractor for payments related to the illegal computer software.

R. Questions

Any employee having questions about this policy may address them to his or her supervisor, and the contractor to their COR.

Attachment A (Executive Order 13103)

[Federal Register: October 5, 1998 (Volume 63, Number 192)]
[Presidential Documents]
[Page 53273-53274]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr05oc98-130]

Presidential Documents

63 F. R. 53273

Executive Order 13103 of September 30, 1998

Computer Software Piracy

The United States Government is the world's largest purchaser of computer-related services and equipment, purchasing more than $20 billion annually. At a time when a critical component in discussions with our international trading partners concerns their efforts to combat piracy of computer software and other intellectual property, it is incumbent on the United States to ensure that its own practices as a purchaser and user of computer software are beyond reproach. Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. It shall be the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of Federal law, including the Copyright Act.

(a) Each agency shall adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.

(b) 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:

(1) preparing agency inventories of the software present on its computers;

(2) determining what computer software the agency has the authorization to use; and

(3) developing and maintaining adequate recordkeeping systems.

(c) Contractors and recipients of Federal financial assistance, including recipients of grants and loan guarantee assistance, should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. If agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors or recipients may affect the integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law.

(d) Executive agencies shall cooperate fully in implementing this order and shall share information as appropriate that may be useful in combating the use of computer software in violation of applicable copyright laws.

Sec. 2. Responsibilities of Agency Heads. In connection with the acquisition and use of computer software, the head of each executive agency shall:

(a) ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency's computers;

63 F. R. 53274

(b) utilize performance measures as recommended by the Chief Information Officers Council pursuant to section 3 of this order to assess the agency's compliance with this order;

(c) educate appropriate agency personnel regarding copyrights protecting computer software and the policies and procedures adopted by the agency to honor them; and

(d) ensure that the policies, procedures, and practices of the agency related to copyrights protecting computer software are adequate and fully implement the policies set forth in this order.

Sec. 3. Chief Information Officers Council. The Chief Information Officers Council (``Council'') established by section 3 of Executive Order No. 13011 of July 16, 1996, shall be the principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software. The Council shall provide advice and make recommendations to executive agencies and to the Office of Management and Budget regarding appropriate government-wide measures to carry out this order. The Council shall issue its initial recommendations within 6 months of the date of this order.

Sec. 4. Office of Management and Budget. The Director of the Office of Management and Budget, in carrying out responsibilities under the Clinger-Cohen Act, shall utilize appropriate oversight mechanisms to foster agency compliance with the policies set forth in this order. In carrying out these responsibilities, the Director shall consider any recommendations made by the Council under section 3 of this order regarding practices and policies to be instituted on a government-wide basis to carry out this order.

Sec. 5. Definition. ``Executive agency'' and ``agency'' have the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

Sec. 6. National Security. In the interest of national security, nothing in this order shall be construed to require the disclosure of intelligence sources or methods or to otherwise impair the authority of those agencies listed at 50 U.S. 401a(4) to carry out intelligence activities.

Sec. 7. Law Enforcement Activities. Nothing in this order shall be construed to require the disclosure of law enforcement investigative sources or methods or to prohibit or otherwise impair any lawful investigative or protective activity undertaken for or by any officer, agent, or employee of the United States or any person acting pursuant to a contract or other agreement with such entities.

Sec. 8. Scope. Nothing in this order shall be construed to limit or otherwise affect the interpretation, application, or operation of 28 U.S.C. 1498.

Sec. 9. Judicial Review. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, at law or equity by a party against the United States, its agencies or

instrumentalities, its officers or employees, or any other person.

/s/ William J. Clinton

THE WHITE HOUSE,

September 30, 1998.

[FR Doc. 98-26799
Filed 10-2-98; 8:45 am]