OFFICE OF
THE INSPECTOR GENERAL

U.S. NUCLEAR
REGULATORY COMMISSION

Review of NRC's Accountability
and Control of Software

OIG-02-A-02 October 26, 2001

AUDIT REPORT

All publicly available OIG reports (including this report) are accessible through NRC's website at:
http://www.nrc.gov/NRC/OIG/index.html

October 26, 2001

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum/**RA**/
Assistant Inspector General for Audits

SUBJECT: REVIEW OF NRC'S ACCOUNTABILITY AND CONTROL OF SOFTWARE (OIG-02-A-02)

Attached is the Office of the Inspector General's audit report titled, *Review of NRC's Accountability and Control of Software*.

This report reflects the results of our review to determine whether NRC's policies governing the control of software and software licensing agreements comply with applicable laws and regulations, and whether management controls are adequate to account for software and ensure that software is properly licensed. Executive Order (EO) 13103, *Computer Software Piracy*, requires all executive agencies to adopt policies and procedures to promote legal software use and proper software management. The review determined that NRC is not in compliance with the EO because its policies (management directives) and its procedures (management controls) do not address the full scope of the EO's requirements. As a result, NRC needs to incorporate EO requirements into its Management Directives System and implement measures to carry out the EO.

At an exit conference held on October 17, 2001, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions, which have been incorporated where appropriate.

If you have any questions, please contact Tony Lipuma at 415-5910 or me at 415-5915.

Attachments: As stated

cc: John Craig, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
B. Garrick, ACNW
D. Powers, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
S. Reiter, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
R. Borchardt, NRR
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
M. Virgilio, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, OSP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, RES
J. Johnson, NRR
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

EXECUTIVE SUMMARY

BACKGROUND

On September 30, 1998, the President signed Executive Order (EO)13103, *Computer Software Piracy*, requiring all executive agencies to adopt policies and procedures to promote legal software use and proper software management. EO 13103 also directed the Federal Chief Information Officers (CIO) Council to improve agency practices concerning acquisition and use of software, and combating the use of unauthorized software. In August 1999, the CIO Council published agency guidelines to promote legal software usage.

PURPOSE

The objectives of the audit were to determine whether the U.S. Nuclear Regulatory Commission's (NRC) (1) policies governing the accountability and control of software and software licensing agreements comply with applicable laws and regulations, and (2) management controls are adequate to account for software and ensure that software is properly licensed.

RESULTS IN BRIEF

NRC is not in compliance with EO 13103. NRC's policies (management directives) and its procedures (management controls) do not address the full scope of EO 13103's requirements because (1) NRC focused its actions on personal use, not *all uses* of software, and (2) the agency planned to change the business approach for its information technology resources. As a result, NRC has not conducted an initial assessment of its software, established a baseline for software inventory, or determined if all software on agency computers is authorized. The lack of adequate policies and procedures leaves the NRC, its employees, and its contractors vulnerable to the consequences of unauthorized software use -- which may include fines and imprisonment.

RECOMMENDATIONS

This report makes six recommendations to the Executive Director for Operations to improve NRC's accountability and control of software and respective licensing agreements. Recommendations can be found at page 5 of this report.

AGENCY COMMENTS

At an exit conference held on October 17, 2001, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions, which have been incorporated where appropriate.

[Page intentionally left blank.]

ABBREVIATIONS AND ACRONYMS

CIO	Chief Information Officer
EO	Executive Order
MD	Management Directive
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

On September 30, 1998, the President signed Executive Order (EO) 13103, *Computer Software Piracy*, requiring all executive agencies to ensure compliance with applicable copyright laws. EO 13103 also directed the Federal Chief Information Officers (CIO) Council to advise and recommend to executive agencies and the Office of Management and Budget "government-wide measures to carry out this order." Appendix B contains the full text of EO 13103.

In August 1999, the CIO Council adopted guidelines for implementing EO 13103, including recommended software management practices (see Appendix C). The General Services Administration then distributed these guidelines to Government agencies.

Computer software is protected by Federal copyright law,[1] which requires users of a particular program to have a software licensing agreement[2] authorizing its use. Under U.S. copyright law, the copying of a copyrighted work without the permission of its author may subject the copier to civil and criminal penalties.[3] For example, in May 2001, a Federal jury in Chicago returned a guilty verdict involving software piracy conspiracy. Individuals conspired to infringe the copyright of more than 5,000 computer software programs that were available through an Internet site. The pirated software had a retail value in excess of $1 million. The civil penalties for copyright infringement include up to a $150,000 fine for each work infringed. Additionally, depending on the circumstances, criminal penalties could be imposed.

As of September 30, 2000, the U.S. Nuclear Regulatory Commission (NRC) had capitalized software with a value of more than $53.1 million with an additional $7.738 million representing software under development.[4] Financial data for noncapitalized software (valued under $50,000) is not available because NRC does track all software or its value.

[1] Copyright Law is contained in Title 17 of the United States Code. The Copyright Revision Act of 1976 (Public Law 94-553), effective January 1, 1978, was amended in 1980 to include computer software under the category of "literary works."

[2] A software publisher's license typically restricts copying of software to specific conditions.

[3] 18 U.S.C. 2318, 2319 and 2319A.

[4] *Independent Auditors' Report and Principal Statements for the Year Ended September 30, 2000*, OIG-01-A-06/March 1, 2001.

II. PURPOSE

The objectives of the audit were to determine whether the NRC's (1) policies governing the accountability and control of software and software licensing agreements comply with applicable laws and regulations, and (2) management controls are adequate to account for software and ensure that software is properly licensed.

III. FINDING

A. NRC IS NOT IN COMPLIANCE WITH EXECUTIVE ORDER 13103

NRC is not in compliance with EO 13103, which requires executive agencies to comply with applicable Federal copyright laws and with the CIO Council recommended software management practices. NRC's policies (management directives) and its procedures (management controls) do not address the full scope of EO 13103 requirements because: (1) NRC focused its actions on personal use, not *all uses* of software, such as official business use; and (2) the agency planned to change the business approach for its information technology resources. As a result, NRC has not conducted an initial assessment of its software, established a baseline for software inventory, or determined if all software on agency computers is authorized. The lack of adequate policies and procedures leaves the NRC, its employees, and its contractors vulnerable to the consequences of unauthorized software use -- which may include fines and imprisonment.

NRC's Management Directives Do Not Address the Full Scope of Executive Order 13103

Management Directive (MD) 1.1, *NRC Management Directives System*, establishes the agency's management directives system as the basis for communicating "NRC policies, requirements, and procedures necessary for the agency to comply with Executive orders, pertinent laws, regulations, and the circulars and directives of other Federal agencies." Thus, the management directives system is the appropriate vehicle to address EO 13103's requirements.

On May 9, 2001, NRC issued MD 2.7, *Personal Use of Information Technology*, which addresses some of the EO's requirements. However, the EO does not focus on just personal use; it addresses *all* uses of software, as does the CIO Council's implementing guidelines.

MD 2.7 defines personal use as "[a]n employee's activity that is conducted for purposes other than accomplishing official or otherwise authorized activity."

NRC permits employees limited use of agency information technology (including software) for personal needs if the use does not interfere with official business and involves minimal additional expense. This directive details inappropriate personal use, some of which corresponds to the EO's admonition against inappropriate use. Employees are admonished against "unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software." Although MD 2.7 addresses personal use, it does not address *all* uses of software. For example, it does not address government purchased software (under a single license) that might be installed at multiple locations, or employee purchased software used for official activities.

To fully comply with EO 13103, NRC's management directives must address all types of software usage.

Agency's Software Management Controls Do Not Implement the CIO Council's Guidelines

As required, the CIO Council established guidelines to implement EO 13103 in August 1999. The guidelines recommended that "Each Federal agency should consider these or similar steps to ensure agency compliance" with EO 13103. The guidelines provide that agency CIOs should be assigned overall responsibility for developing and implementing plans to ensure compliance.

The CIO Council's guidance also recommended that agency CIOs review whether existing procedures promote legal software use and proper software management. Suggested procedures in the CIO Council's guidelines include (1) making an initial assessment of the agency's existing policies and practices with respect to the use and management of software, (2) establishing an initial baseline of the agency's software to assess whether the agency's software usage complies with applicable software licenses,[5] (3) preparing agency inventories of software present on its computers, (4) determining what software the agency is authorized to use, and (5) developing and maintaining adequate record keeping systems. The entire text of the CIO Council guidelines is shown in Appendix C.

As stated, MD 2.7 only addresses personal use policy and does not reference additional policies or procedures that implement the CIO Council guidelines. For example, NRC has not conducted an initial assessment, established a baseline for software inventory, or determined if all software on agency computers is authorized.

[5] This should include software on individual computers and software accessed through the agency networks. Upon completion of the initial baseline, any unauthorized copies of software should be (1) properly licensed or (2) destroyed and replaced with licensed copies.

Inadequate controls over agency software are exacerbated by the agency's procedures for permitting individual offices to purchase and *control* software. Neither the Office of the Chief Information Officer (OCIO) nor other NRC offices adequately control agency software. The Office of the Inspector General's (OIG's) discussions with representatives from NRC's larger offices disclosed that none maintain a software inventory that accounts for all licensed software installed on their computers.

Implementation Focused On Personal Use and a Changing Information Technology Environment

OCIO staff stated that the agency has not fully implemented EO 13103 because OCIO (1) focused on personal software use (MD 2.7), which they considered to be a high priority area; and (2) planned to change its business approach for managing NRC information technology resources.

OCIO staff acknowledged that MD 2.7 is the primary policy directive that addresses segments of EO 13103's requirements. They stated that MD 12.5, *NRC Automated Information Systems Security Program*, revised February 1, 1999, also addresses some of the concepts contained in the EO. However, OCIO staff acknowledged that the management directives system should contain more policy guidance to fully implement the EO.

OCIO staff also advised that EO 13103 has not been fully implemented because of the forthcoming seat management contract. Under seat management, an agency contractor procures and manages hardware, software, and related support services.

OCIO staff was advised that OIG's review of the statement of work for the proposed seat management contract determined that the contract did not clearly describe a contractor's responsibility for meeting the EO's requirements. OCIO staff stated that meeting these requirements will be a shared responsibility of the agency and the prospective contractor. Because neither the division of responsibility nor the need to meet EO 13103's requirements are clear, OIG recommended that the contract be specific about the duties assigned to the successful contractor. OIG provided these concerns and a recommendation to NRC's CIO in a memorandum dated August 31, 2001 (see Appendix D). The CIO's response can be found in Appendix E.

OCIO staff advised that, while improvements are needed, they are sensitive to honoring software licensing agreements and using only legal software. OCIO staff concluded that the MDs should include the full spectrum of controls established in EO 13103 and the CIO Council's implementing guidance. They advised OIG that additional policy and guidance will be forthcoming.

Inadequate Policies and Controls Put the Agency At Risk

Because NRC's guidance to date is directed at personal software usage, NRC is not in compliance with EO 13103. Neither OCIO nor individual offices have adequate software controls that meet the EO's requirements. As a result, the agency does not adequately safeguard its property or know its degree of compliance with software licenses.

Inadequate controls can lead to loss or misuse of agency property. Furthermore, use of unauthorized software could tarnish the agency's reputation and subject it, its employees, and its contractors to significant legal penalties, such as fines or imprisonment. In addition, NRC could be required to delete any unlicensed software from its computer systems and purchase replacement copies.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Incorporate the requirements of Executive Order 13103, *Computer Software Piracy*, and the provisions of the Chief Information Officers Council August 1999 guidance into NRC's Management Directives System.

2. Issue interim guidance on software use until NRC's Management Directives System is updated.

3. Institute property management accountability and controls for all software.

4. Incorporate Executive Order 13103, *Computer Software Piracy*, provisions into the seat management contract.

5. Develop procedures for monitoring compliance with Executive Order 13103, *Computer Software Piracy*.

6. Establish a documented inventory of all authorized software on agency computers and remove all unauthorized software.

[Page intentionally left blank.]

SCOPE AND METHODOLOGY

To accomplish the audit objectives, the Office of the Inspector General (OIG) reviewed and analyzed pertinent laws, regulations, authoritative guidance, and prior agency OIG and U.S. General Accounting Office reports. In addition, OIG identified, analyzed, and compared NRC guidance with the aforementioned criteria. OIG interviewed NRC staff to identify agency policies governing the accountability and control of software and compliance with licensing agreements, and to determine current issues, problems, or known deficiencies. OIG interviewed staff in the Offices of the Chief Information Officer, Chief Financial Officer, Nuclear Reactor Regulation, Nuclear Material Safety and Safeguards, and Administration to determine responsibilities for purchasing and controlling software and licensing agreements.

Management controls relevant to the audit were reviewed and analyzed. Throughout the review, auditors were aware of the possibility or existence of fraud, waste or misuse in the program under review. OIG conducted the audit in accordance with Generally Accepted Government Auditing Standards from June through August 2001.

The major contributors to this report were Anthony Lipuma, Team Leader; Steven Zane, Audit Manager; and Michael Steinberg, Senior Auditor.

[Page intentionally left blank.]

EXECUTIVE ORDER 13103, *COMPUTER SOFTWARE PIRACY*

THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release October 1, 1998

EXECUTIVE ORDER
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 record keeping 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; (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.

WILLIAM J. CLINTON
THE WHITE HOUSE,
September 30, 1998.

[Page intentionally left blank.]

CHIEF INFORMATION OFFICERS COUNCIL GUIDELINES

Guidelines for Implementing the
Executive Order 13103
on
Computer Software Piracy
Federal CIO Council
Approved August, 1999
TABLE OF CONTENTS

Guidelines for
Implementing the Executive Order
on
Computer Software Piracy

These Guidelines are issued by the CIO Council pursuant to the Executive Order on Computer Software Piracy (Executive Order 13103 — September 30, 1998). The Order requires the Council to provide advice and make recommendations to executive agencies and to the Office of Management and Budget on appropriate government-wide measures to carry out the Order. In developing these Guidelines, the Council has attempted to balance each agency's obligation to comply with the directives of the Order against the need for flexibility in developing agency practices and procedures. Accordingly, the Guidelines suggest general best practices that promote legal use of software without imposing rigid requirements to achieve this goal.
Note: **A software management toolkit with model policies and training materials will be published separately to assist agencies with implementation of the Executive Order.**

I INTRODUCTION

A. Background

As the nation's largest consumer of software, the U.S. Government has an essential role to play in setting an example for the nation as a lawful user of computer software. Computer software is protected by Federal copyright law, which requires users of a particular software program to have a license authorizing such use. To provide guidance to Federal agencies in fulfilling this role, President Clinton issued the Executive Order on Computer Software Piracy (Executive Order 13103 -September 30, 1998) (Order), which seeks to:

- Ensure that executive agencies of the U.S. Government acquire, reproduce, distribute, transmit, and use computer software in compliance with international treaty obligations and federal law, including the Copyright Act;
- Ensure that executive agencies maintain only legal software on their computers and computer networks; and
- Ensure that Government contractors and recipients of grants and other Federal funding do not use such funds to acquire, create, operate or maintain computer software in violation of applicable copyright laws.

B. Summary of Executive Order Requirements

President Clinton signed the Executive Order on Computer Software Piracy on September 30, 1998. The Order sets forth the Government's policy against the use, acquisition, reproduction, distribution, and transmission of computer software that violates applicable copyright laws. To implement this policy, the Order ***directs*** each executive agency to:

- Adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws;

- 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:
  - preparing agency inventories of the software present on its computers;
  - determining what computer software the agency has authorization to use; and
  - developing and maintaining adequate record keeping systems.
- Take appropriate measures, including for example the use of certifications or written assurances, in the event the agency becomes aware that contractors or recipients of Federal financial assistance are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determines that such actions may affect the integrity of the agency's contracting and Federal financial assistance processes;
- Cooperate fully in implementing the Order and share information that may be useful in combating the use of computer software in violation of applicable copyright laws;
- Educate appropriate agency personnel regarding software copyrights and the policies and procedures adopted by the agency to honor them; and
- 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 the Order.

  The Executive Order also directs the Office of Management and Budget to use its oversight mechanisms to foster compliance with the Order.

II RECOMMENDED SOFTWARE MANAGEMENT PRACTICES

Each Federal agency should consider these or similar steps to ensure agency compliance with the Order:

A. Assign Responsibilities

Assign to the Chief Information Officer (CIO) overall responsibility for developing and implementing a plan to ensure agency compliance with the Order utilizing resources from throughout the organization. The CIO should look to these Guidelines as a resource in developing such a plan. Other partner organizations within the agency may be needed to properly implement this Executive Order. For example, the CIO may wish to partner with the agency's Inspector General to conduct the initial assessment described below in paragraph B; the Procurement Executive to develop and implement the software management policies referenced in paragraph C; and Human Resources to develop and implement the training program referenced in paragraph D. The CIO may delegate specific tasks to appropriate personnel within the agency, provided that he or she exercises sufficient supervision to ensure that such tasks are completed in a satisfactory manner.

3. Direct your CIO to develop performance measures to assess the agency's compliance with the Order.

B. Initial Assessment. The CIO should coordinate through qualified personnel or an outside contractor an initial assessment of the agency's existing policies and practices with respect to the use and management of computer software. The purpose of the assessment is to help the agency evaluate its current state of compliance with the Order and to identify any additional measures needed to achieve compliance. The assessment may vary from agency to agency. However, each agency should, at a minimum, review whether existing policies and procedures promote legal software use and proper software management (as described below in paragraph 1). In addition, each agency should, to the extent feasible, establish the initial software baseline described in paragraph 2, particularly if agency policies and procedures with respect to software use and management are found to be deficient in any respect:

1. Review and identify deficiencies in existing policies and procedures, including procedures for acquiring and installing software, storage and disposition of software and licenses, and software training.

2. Establish an initial baseline of the agency's software (including copies installed on individual computers and accessed through agency networks) to assess whether the agency's software usage complies with applicable software licenses. The agency may use a sampling approach to assess its existing software management policies and practices. Upon completion of the initial baseline, any unauthorized copies of software should be (i) properly licensed or (ii) destroyed and replaced with licensed copies.

C. Software Management Policy. Develop a software management policy on the acquisition and use of software by the agency and its employees.

1. Adopt a policy prohibiting the use or installation of software by agency employees for which the agency lacks appropriate licenses (unless such software is properly licensed to the employee and used in accordance with agency policy).

2. Adopt a software acquisition policy to guard against the acquisition of counterfeit software or software that violates licensing restrictions. The software acquisition policy should, among other things, require the following procedures:
   a. Educate employees authorized to acquire software on the Agency's acquisition procedures.
   b. To the extent feasible and consistent with agency acquisition procedures, standardize the agency's policy of acquisition of software.
   c. Obtain from software resellers (i) proper licenses for any software supplied to the agency, or (ii) other information from which the agency can determine that its use of such software is validly licensed by the copyright holder.
   d. Purchase software from reputable resellers.

3. To the extent feasible and consistent with agency acquisition procedures, adopt software installation and distribution procedures to ensure that software: (i) originates from the office(s) designated by the agency to acquire new software; (ii) is approved by those office(s); or (iii) meets Agency IT architecture and standards requirements.

4. Establish and maintain a record keeping system for documentation and materials evidencing legal use of the agency's software, including, for example, original software licenses, certificates of authenticity, purchase invoices, and copy of completed registration card. Consider the use of software management computer programs to automate such record keeping. If feasible, store such records, as well as any original software media (e.g., CD-ROMs or diskettes), in secure, designated location(s) within the agency.

5. Include in the agency's software management policy provisions concerning the downloading of software from the Internet by agency employees, the use of user-owned software on agency computers, the use of agency-owned software from home or remote computers, and the decommissioning of agency computers. Ensure that such uses of software comply with applicable licenses and agency policy.

6. Include in the agency's software management policy information concerning the authorities to whom employees can direct questions about the policy and report possible violations of the policy.

7. Develop and adopt procedures for monitoring compliance with the software management policy, addressing reports and incidents of alleged violations of the policy, and disciplining employees who knowingly violate the policy or Federal copyright laws.

D. **Training.** Develop a training program for existing and new employees.

   1. Existing Employees
      a. Amend employee handbook to include the agency's software management policy, and distribute the updated handbook to all employees.
      b. Provide training on the agency's software management policy for existing employees to inform them of the types of software piracy, how to detect and prevent piracy, how to implement the software use policy, and consequences of violating the policy. Such training may be conducted as a separate seminar or as a part of existing training programs.
      c. Circulate reminders of the agency's software management policy on a regular basis (at least annually) or remind employees of the policy in other ways (at least annually), for example, through notices in agency newsletters.
      d. Inform employees where they can get additional information on the agency's software management policy and software piracy prevention.

2. New Employees
   a. Provide each new employee an employee handbook that includes the agency's software management policy.
   b. Train new employees during their initial agency orientation on how to comply with the agency's software management policy.

E. **Periodic Inspections and Assessments.** Develop a system (possibly in conjunction with the IG or other agency assessment tool) for periodic and random inspections and assessments to evaluate the effectiveness of the software management policy. (A tool kit of helpful practices is to be published separately to assist agencies with implementation).

III OTHER REQUIREMENTS

Software Use by Government Contractors and Recipients of Federal Funds. The Executive Order requires government contractors and recipients of Federal grants and loans to 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 an agency becomes aware that contractors or recipients are using Federal funds to acquire, operate, or maintain unlicensed software and determine that such actions may affect the integrity of the agency's contracting and financial assistance processes, the agency is required to "take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law."

NOTE: Guidance will be issued separately with respect to these requirements of the Executive Order.

MEMORANDUM TO NRC'S CHIEF INFORMATION OFFICER

August 31, 2001

MEMORANDUM TO: Stuart E. Reiter
Chief Information Officer

FROM: Stephen D. Dingbaum/**RA**/
Assistant Inspector General for Audits

SUBJECT: INFORMATION TECHNOLOGY SEAT MANAGEMENT CONTRACT

On August 23, 2001, OIG met with Office of the Chief Information Officer (OCIO) staff (Messrs. Schaeffer, Shields and Kee) to discuss issues related to our ongoing audit of NRC's software and licensing agreements. The purpose of this memorandum is advise you of an issue that needs immediate attention.

During the August 23rd meeting, we discussed the forthcoming seat management contract and how it addresses the requirements contained in Executive Order (EO) 13103, *Computer Software Piracy*. OCIO staff stated that the agency plans to award this contract in early September. OIG advised the OCIO staff that the Statement of Work for the proposed contract does not clearly describe a contractor's responsibility for meeting the EO's requirements.

The OCIO staff advised that meeting these requirements will be a shared responsibility of OCIO and the selected contractor. Because neither this division of responsibility or need to meet the EO's requirements are clear, OIG recommends that the seat management contract be specific about the duties assigned to the successful vendor. This action is needed to comply with the provisions of the EO and to protect the NRC, its employees, and the vendor from the potential consequences related to using software that is not properly licensed.

If you have any questions, please contact Tony Lipuma at 415-5910 or me at 415-5915.

Attachments: As stated

cc: William D. Travers, EDO

[Page intentionally left blank.]

MEMORANDUM FROM NRC'S CHIEF INFORMATION OFFICER

October 16, 2001

MEMORANDUM TO: Stephen Dingbaum
Assistant Inspector General for Audits
Office of the Inspector General

FROM: Stuart Reiter/**RA**/
Chief Information Officer

SUBJECT: INFORMATION TECHNOLOGY SEAT MANAGEMENT CONTRACT

This is in response to your memorandum dated August 31, 2001, subject as above. As discussed in the August 23, 2001 meeting with Tony Lipuma, we will work with the Office of the Inspector General (OIG) to address the requirements contained in Executive Order (EO) 13103, *Computer Software Piracy*. The Office of the Chief Information Officer has policies and procedures in place to address some of the requirements of the EO, and will work with the agency to modify and enhance them as necessary. We would appreciate any recommendations the OIG can provide on implementing the requirements of the EO.

The Statement of Work for the NRC Infrastructure Services and Support Contract was awarded on September 28, 2001 under the GSA Seat Management Contract. It requires the contractor to track the installation, location, related license, warranty, maintenance and service records for all hardware and software provided under the order and hardware connected to it, including NRC-owned and personally-owned hardware and software. However, the major requirements in this area are for the vendor to provide an inventory of software installed on agency hardware and maintain licenses for software they manage, acquire, and/or install under the Statement of Work.

The next step will be for the contractor to develop a detailed Concept of Operations for NRC approval that will specify how they will meet agency inventory, license management, and other operational requirements. Please contact James B. Schaeffer (415-8720, JBS) if you have any questions or to arrange any assistance you may be able to provide.

cc: W. Travers, EDO