# Audit Report

OFFICE OF THE INSPECTOR GENERAL

## CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE AT THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

Report Number 92-134 September 9, 1992

**Department of Defense**

**The following acronyms are used in this report.**

DTSA.....Defense Technology Security Administration
IBM.....International Business Machines Corporation

**INSPECTOR GENERAL**
**DEPARTMENT OF DEFENSE**
**400 ARMY NAVY DRIVE**
**ARLINGTON, VIRGINIA 22202-2884**

September 9, 1992

MEMORANDUM FOR DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

SUBJECT: Audit Report on Controls Over Copyrighted Computer Software at the Defense Technology Security Administration (Report No. 92-134)

This final report is provided for your information and use. The report addresses unauthorized use of copyrighted computer software on computers within the Defense Technology Security Administration. The audit was performed as part of our overall Audit of Controls Over Copyrighted Computer Software.

Comments on a draft of this report conformed to the requirements of DoD Directive 7650.3, and there are no unresolved issues. Therefore, no additional comments are required.

The courtesies extended to the audit staff are appreciated. If you have any questions on this audit, please contact Mr. Harrell D. Spoons on (703) 692-2846 or Mr. Marvin L. Peek on (703) 692-2856.

Robert J. Lieberman
Robert J. Lieberman
Assistant Inspector General
for Auditing

cc:
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Office of the Inspector General

**AUDIT REPORT NO.** 92-134 September 9, 1992
(Project No. 2RF-5004.02)

# CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE AT THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

## EXECUTIVE SUMMARY


**Introduction.** The Defense Technology Security Administration (DTSA), with an annual operating budget of $8.6 million, administers the DoD Trade Security Program. This mission includes reviewing and processing export license applications and ensuring that the security policy for DoD technology is implemented. DTSA was included in our ongoing audit of Controls Over Copyrighted Computer Software because of a DoD Hotline allegation that DTSA was illegally duplicating and installing software on its computers.

**Objective.** The audit objective was to determine whether DTSA was using copyrighted software programs in accordance with licensing agreements. We also evaluated applicable internal controls.

**Audit Results.** Of 133 computers tested, 123 had at least 1 copyrighted software program installed without documentation to show it had been legally acquired. Overall, we found 640 copies of undocumented, installed software with an estimated retail value of $72,000. Use of unlicensed software denies vendors their rightful revenues.

**Internal Controls.** Although DTSA had issued guidance to control and account for computer software, the policies were neither effective nor enforced. The controls we assessed are described in Part I of the report, and the finding provides details on the weaknesses.

**Potential Benefits of Audit.** No monetary benefits are associated with the recommendations in this report. Implementation of the recommendations will ensure that DTSA complies with licensing agreements for copyrighted software and will prevent liability to DoD for noncompliance with copyright laws. A summary of benefits resulting from this audit is in Appendix A.

**Summary of Recommendations.** We recommended removing unauthorized software programs from DTSA's computers and establishing internal controls over the acquisition and use of copyrighted computer software.

**Management Comments.** The Director, Defense Technology Security Administration, concurred with the recommendations, and there are no unresolved issues. The text of his comments is in Part IV of this report.

## TABLE OF CONTENTS


| | Page |
|---|---|
| TRANSMITTAL MEMORANDUM | |
| EXECUTIVE SUMMARY | i |
| PART I - INTRODUCTION | 1 |
| Background | 1 |
| Objectives | 1 |
| Scope | 1 |
| Internal Controls | 2 |
| Prior Audits and Other Reviews | 2 |
| PART II - FINDING AND RECOMMENDATIONS | 3 |
| Use of Copyrighted Software | 3 |
| PART III - ADDITIONAL INFORMATION | 9 |
| Appendix A - Summary of Potential Benefits Resulting from Audit | 11 |
| Appendix B - Activities Visited or Contacted | 13 |
| Appendix C - Report Distribution | 15 |
| PART IV - MANAGEMENT COMMENTS | 17 |
| Director, Defense Technology Security Administration | 19 |



This report was prepared by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, DoD. Copies of the report can be obtained from the Audit Planning and Technical Support Directorate at (703) 614-6303.

## PART I - INTRODUCTION

### Background

The Defense Technology Security Administration (DTSA) is under the direction and control of the Under Secretary of Defense for Policy. The Deputy Under Secretary of Defense (Trade Security Policy) serves as the Director, DTSA. DoD Directive 5105.51, "Defense Technology Security Administration," May 10, 1985, charters DTSA to administer the DoD Technology Security Program with the mission to review the international transfer of defense-related technology, goods, services, and munitions consistent with U.S. foreign policy and national security objectives. This mission includes reviewing and processing applications for export licenses. At the time of the audit, DTSA was authorized 136 employees and had an FY 1992 operation and maintenance budget of $8.6 million.

On January 28, 1992, an anonymous allegation was forwarded to the Inspector General, DoD, stating that DTSA had copied and installed commercial software programs in violation of licensing agreements and copyright laws. Also, an article appeared in the February 6, 1992, issue of Washington Technology reporting that DTSA had "pirated" computer software from various companies.

U.S.C., title 17, section 106, gives copyright owners exclusive rights to reproduce and distribute their material, and section 504 states that copyright infringers can be held liable for damages to the copyright owner. Defense Federal Acquisition Regulation Supplement, paragraph 252.227-7013 prohibits unauthorized distribution or copying of commercially-developed software without written consent from the supplier.

### Objectives

The objective of the audit was to determine whether DTSA had installed commercial software programs in accordance with licensing agreements and copyrights. We also evaluated policies and procedures for the control and accountability of microcomputer software in DTSA.

### Scope

DTSA had 150 IBM-compatible[1] microcomputers and 38 other microcomputers. We examined files installed on 133 of DTSA's

---

1. IBM is a registered trademark of the International Business Machines Corporation.

150 IBM-compatible computers to determine which commercial software programs were installed. We physically examined 22 computers to identify the software installed, and we examined software files DTSA personnel extracted from the other 111 computers. We judgmentally selected a sample of 50 software programs purchased by or found installed on DTSA computers for detailed review. We examined available computer software procurement and inventory records, dated from October 1988 through February 1992, to determine the number of copies of software programs authorized to be installed on DTSA computers. We also contacted software vendors to verify information when necessary. In addition, we evaluated internal controls over the installation and operation of software on DTSA's computers.

This program audit was made from March through April 1992. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD, and accordingly included such tests of internal controls as were considered necessary. Activities visited or contacted are listed in Appendix B.

**Internal Controls**

We examined controls over the accountability and installation of computer software and found that controls were neither effective nor enforced. However, we did not consider these weaknesses material as defined by Public Law 97-255, Office of Management and Budget Circular A-123, and DoD Directive 5010.38. Implementation of Recommendation 2. in this report will correct the weaknesses. Details on the weaknesses are discussed in the finding in Part II of this report.

**Prior Audits and Other Reviews**

The Assistant Inspector General for Inspections, DoD, conducted an inspection of DTSA during July and August 1991 and issued Report No. 92-INS-08, "Defense Technology Security Administration Inspection Report," on April 17, 1992. Compliance with commercial software licensing agreements was not covered in the inspection. However, the overall evaluation indicated that internal management controls and oversight within DTSA were inadequate.

## PART II - FINDING AND RECOMMENDATIONS

### USE OF COPYRIGHTED SOFTWARE

Of 133 computers tested, 123 had at least 1 copyrighted software program installed without documentation to show it had been legally acquired. Overall, we found 640 copies of undocumented software installed with an estimated retail value of $72,000. The unauthorized copies were installed because controls over the use of microcomputer software were not effective and because DTSA management did not ensure compliance with licensing and copyright restrictions. Improper use of copyrighted computer software contravenes Federal law and denies vendors their rightful revenues.

### DISCUSSION OF DETAILS

#### Background

Software vendors attempt to control unauthorized use of their products through licensing agreements that invoke the protection available under copyright statutes. The specific licensing agreement for each software product is explained in documentation that accompanies the system disks that enable the user to install and operate the software program on a computer. Licensing agreements for software sold to U.S. Government activities typically restrict the use of the software program to a single computer. In some instances, an activity may purchase a "site license" or a license to use a software program on a local area network of computers. Such licenses permit an activity to use the covered software program on the number of computers specified in the agreement.

#### DTSA Software Management

The Director, Information Resource Management, is responsible for software management and for providing technical support for automated systems within DTSA. A contractor assisted DTSA with the installation of computer software programs and other aspects of software management. Although Information Resource Management personnel are responsible for the installation of computer software, it is difficult, if not impossible, to prevent users from installing personally owned or borrowed software programs on their assigned computers.

DTSA's Administrative Instruction No. 18, "Guidelines for Installation and Operation of Software," published in July 1988

and updated on November 20, 1991, establishes policy for the control and accountability of software. The instruction provides that:

o No software will be used on DTSA workstations without approval from the Director, Information Resource Management.

o Only copyrighted software licensed to DTSA may be installed on DTSA equipment. All use shall be in full compliance with software copyrights.

o No entertainment software programs will be used on DTSA equipment.

The Director, Information Resource Management, stated that his approval was generally not requested before software was installed on computers. Except for occasional references to software installation in the contractor's biweekly status reports, records were not maintained by either the contractor or DTSA personnel to show what software had been installed on DTSA computers.

The DTSA had inventoried software manuals and installation disks during November 1989 through January 1990, and in June 1990, began to maintain a log of software received. However, an inventory of software installed on each computer was not maintained, although the inventory is required by the DTSA Automated Information System Security Plan, May 22, 1991.

**Software Installed on Computers**

**Excessive copies**. For 19 of the 50 software programs sampled, documentation was available to support the acquisition of at least 1 copy of software found on DTSA computers. Collectively, there were 645 copies of the 19 software programs; however, only 266 copies were properly licensed, while 379 copies were in excess of licensing agreements. Examples of the use of excess copies follow.

In May 1990, the DTSA purchased 75 copies of Word Perfect software, costing $11,100, and 74 copies of Word Perfect Office software, costing $5,661. However, we found copies of those programs installed in 123 of the 133 computers examined. At the time of our audit, both products were considered standard software for the IBM-compatible computers used by DTSA. The Director, Information Resource Management, stated that he had verbally approved installing Word Perfect and Word Perfect Office software during FY 1991 on all IBM-compatible computers before sufficient copies were purchased so that DTSA could more effectively perform its mission. He stated he planned to purchase additional copies of the software at the beginning of FY 1992, when sufficient funding was available but did not

document that decision. Documentation showed that the DTSA received funding authority on December 13, 1991, to purchase items, such as computer software. On February 19, 1992, the DTSA ordered 76 copies of Word Perfect software for $11,022 and 75 copies of Word Perfect Office software for $3,126.

Procurement records showed that two copies of a utility program used to back up hard disks had been purchased at $94.50 each. The audit showed that copies of the software were installed in 79 DTSA computers.

Although records showed that 7 copies of a copyrighted data base software program had been purchased, the audit showed that the program was installed on 29 DTSA computers. We were informed that some of the excess copies were installed because DTSA personnel had received training on the use of the software and demanded to use the software, even though sufficient copies had not been purchased.

**Questionable ownership of software**. We found no documentation to show that DTSA had purchased 18 of the 50 software programs in the sample. We found a total of 261 copies of the 18 programs installed on DTSA computers. Some of the software we found is discussed below.

Software products on DTSA computers were identified as personally owned, provided by others, installed by the contractor, or of unknown origin. The products included:

- o a computer graphics program, with an approximate unit cost of $275, installed on 13 computers;

- o an edit utility program, with an approximate unit cost of $48, installed on 73 computers; and

- o a word processing program, with an estimated unit cost of $205, installed on 7 computers.

DTSA purchased 165 adapter cards (PC 2001-EN) with accompanying software from TRW, Incorporated, in three purchases in FY 1988 through FY 1990. The accompanying software was installed on IBM-compatible computers and was considered part of the standard software for the computers. Contractors and DTSA personnel had numerous problems getting the automated systems to work properly using the version of the software provided with the TRW adapter cards. According to contractor and DTSA progress reports in December 1990, TRW provided DTSA an updated version of the installed software. The updated version was installed on 123 of the 133 computers tested in our audit sample. A DTSA automated systems specialist, who worked closely with TRW, stated that TRW field engineers told her the updated version was provided at no cost and could be used on computers already using the older

version. However, documentation on the verbal agreement was not maintained by DTSA or TRW. TRW's standard procedure is to charge customers about $50 for each upgraded version of the software. We do not fault DTSA personnel for installing the updated version of the software without additional payment, if TRW marketing representatives stated the charge was waived; however, the absence of documentation precluded verification that payment was not required.

**Loaned Software**

DTSA purchased and installed 10 copies of a data management software program on two local area networks. Since DTSA was not fully utilizing all 10 copies of the software, DTSA gave a copy of the software and a photocopy of the user manual to one of its contractors in August 1991. When the software vendor learned of the loan in the fall of 1991, it telephoned DTSA to protest the violation of the licensing agreement. On February 20, 1992, DTSA requisitioned an additional copy of the software for $1,144.

**Corrective Actions**

In September 1990, DTSA tasked the software support contractor to develop a Resource Management Data Base System. One of the planned modules of the system included a software management data base. On February 26, 1992, the contractor provided DTSA with a draft software inventory module that could provide reports showing software purchased, the number of legal licenses for each software program, a list of the software installed on each computer, and a list of software acquired that had not been assigned or installed. If unauthorized software is removed from DTSA computers and the planned software inventory data base program is implemented, DTSA should have an effective procedure to account for and control computer software. These actions coupled with periodic internal reviews will ensure integrity of all information systems.

**Conclusion**

DTSA had established policies that, if enforced, should have eliminated unauthorized software from being installed on its computers; however, DTSA's management of copyrighted computer software was ineffective. DTSA management directed or allowed the installation of software programs in violation of software licensing agreements, and documentation for software that may have been licensed was not always maintained. The estimated cost of the undocumented software we found on DTSA computers averaged only about $113 per copy; however, copyrighted software at any cost must be documented to show it was legally acquired. Use of copyrighted software programs in violation of licensing agreements deprives vendors of their rightful revenues.

## RECOMMENDATIONS, MANAGEMENT COMMENTS, AND AUDIT RESPONSE

We recommend that the Director, Defense Technology Security Administration:

1. Identify and remove from the computers each software program for which a licensing agreement has not been purchased.

2. Establish procedures for the acquisition and use of copyrighted computer software to:

a. Maintain a current inventory of the software authorized to be installed on each computer.

b. Periodically review the propriety of software installed on computers.

c. Inform employees of software licensing agreements and copyright restrictions.

d. Provide for disciplinary action if an employee violates a software licensing agreement.

**Management comments.** The Director, DTSA, concurred with the recommendations and stated that copyrighted software programs without adequate documentation had been removed from computers. A copy of DTSA's revised procedures implementing Recommendation 2. was included in the response.

**Audit response.** We consider management's comments to be fully responsive to the recommendations.

## PART III - ADDITIONAL INFORMATION

Appendix A - Summary of Potential Benefits Resulting from Audit

Appendix B - Activities Visited or Contacted

Appendix C - Report Distribution

## APPENDIX A: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

| Recommendation Reference | Description of Benefit | Type of Benefit |
|---|---|---|
| 1. | Compliance with Copyright laws. One-time action to purge unauthorized software from computers | Nonmonetary |
| 2. | Internal Control. Enhances controls over computer software and promotes compliance with licensing agreements. | Nonmonetary |

## APPENDIX B: ACTIVITIES VISITED OR CONTACTED

### Office of the Secretary of Defense

Under Secretary of Defense for Policy
- Deputy Under Secretary of Defense (Trade Security Policy)
- Deputy Under Secretary of Defense (Security Policy)
- Defense Technology Security Administration

Washington Headquarters Services

### Department of the Army

Defense Supply Service - Washington, Administrative Assistant, Office of the Secretary of the Army

### Non-Government

Federal Systems Division, American Telephone and Telegraph, Incorporated
Decision Systems Technologies, Incorporated
Digital Equipment Corporation
Potomac Systems Engineering, Incorporated
Systems Engineering and Development Division, TRW, Incorporated

## APPENDIX C: REPORT DISTRIBUTION

Office of the Secretary of Defense

Under Secretary of Defense for Policy
Defense Technology Security Administration
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant Secretary of Defense (Public Affairs)
Comptroller of the Department of Defense

Department of the Army

Auditor General, Army Audit Agency

Department of the Navy

Auditor General, Naval Audit Service

Department of the Air Force

Auditor General, Air Force Audit Agency

Other Defense Activities

Director, National Security Agency/Central Security Service
Inspector General, Defense Intelligence Agency
Defense Logistics Studies Information Exchange

Non-DoD Activities

Office of Management and Budget
U.S. General Accounting Office
NSIAD Technical Information Center

Chairman and Ranking Minority Member of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Committee on the Judiciary
Senate Subcommittee on Patents, Copyrights, and Trademarks, Committee on the Judiciary
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations

**APPENDIX C: REPORT DISTRIBUTION** (Cont'd)

Non-DoD Activities (Cont'd)

House Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations
House Committee on the Judiciary
House Subcommittee on Courts, Intellectual Property, and the Administration of Justice, Committee on the Judiciary
House Committee on Science, Space, and Technology
House Subcommittee on Science, Research, and Technology, Committee on Science, Space, and Technology
House Permanent Select Committee on Intelligence
House Subcommittee on Oversight and Evaluation, Permanent Select Committee on Intelligence

## PART IV - MANAGEMENT COMMENTS

Director, Defense Technology Security Administration

## DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION COMMENTS

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D C 20301-2000

POLICY

AUG 14 1992

In reply refer to:
I-31428/92

MEMORANDUM FOR DIRECTOR, READINESS AND OPERATIONAL SUPPORT DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on Controls Over Copyrighted Computer Software at the Defense Technology Security Administration (Project No. 2RF-5004.02) - INFORMATION MEMORANDUM

We have carefully reviewed the draft report and accept its recommendations. Since your auditors concluded their on-site work, the Defense Technology Security Administration (DTSA) has removed from its computers all copyrighted software programs for which we had inadequate documentation. We have also supplemented DTSA's procedures to include specific provisions for maintaining a current inventory of authorized software, confirming periodically the authorized software loadings on each computer and informing employees that failure to comply with DTSA's procedures and copyright restrictions will subject them to possible disciplinary action. These supplemental procedures have been included in revised DTSA Administrative Instruction No. 18, a copy of which is attached.

Following its creation in 1985, DTSA made a concerted effort to develop modern automated support systems and a computer literate staff that could effectively exploit them. I wish to emphasize that, well before the audit and in the absence of specific DoD guidance, DTSA recognized the need to implement internal procedures for controls over copyrighted computer software and was in the process of implementing them. The draft report acknowledges that DTSA had established policies in July 1988 that were intended to prevent the installation of software on its computers unless authorized by appropriate staff. Our ability to enforce these policies admittedly had been less than adequate. As the draft points out, "it is difficult, if not impossible, to prevent users from installing personally owned or borrowed software programs on their assigned computers."

Initial manual efforts by DTSA in 1989-1990 to document its software inventory proved to be insufficient. Thus, DTSA tasked its software support contractor in September 1990 to develop a plan to automate inventory procedures to better account for authorized software. While slowed by other high priority projects, the system was mature enough to produce the essential baseline data that enabled your auditors to do their work and, at the same time, allowed us to identify and remove all inadequately documented software.

We concur with the audit report's conclusion that the actions taken by DTSA "will ensure the integrity of all information systems." However, we believe that the policing of our current procedure is very labor intensive and, in the long run, not the most cost-effective means of software control. One of the benefits of our local area network is that it will facilitate enforcement of our software controls. In this connection, since well before the audit, we have been exploring the possibility of acquiring a specialized software program that will block the loading of unauthorized software on individual DTSA computers. Subject to funding availability and the procurement regulations, we hope to identify and purchase such a program within a year.

The draft report does not cite any evidence of willful violation of the copyright laws. Nor has our own internal review revealed any such evidence.

Finally, I wish to acknowledge the professionalism of your audit team. They spent many long hours with our staff learning how DTSA is coping with complex software problems and their constructive interaction led to a sound set of recommendations.

William Rudman

William N. Rudman
Deputy Under Secretary
Trade Security Policy

Attachment
As stated

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D C 20301-2000

AUG 14 1992

POLICY

ADMINISTRATIVE INSTRUCTION NO. 18

SUBJECT: Installation and Operation of Software on DTSA's Defense Export License Tracking and Analysis (DELTA) Workstations

Reference: (a) DODD 5500.7, "Standards of Conduct"
(b) Federal Information Resource Management Regulations (FIRMR)
(c) DTSA Automated Information Systems Security Plan

A. PURPOSE. To establish procedures in accordance with the references (a), (b), and (c) to control software which will be used as standard, support tools and development packages for DTSA and to promulgate security procedures to insure the integrity of information within the DELTA information systems environment.

B. APPLICABILITY. This instruction applies to all employees of the Defense Technology Security Administration (DTSA) to include contractors and consultants who are authorized access to the DTSA microcomputer workstations.

C. POLICY. It is the policy of DTSA to insure the integrity of the classified and unclassified information systems against compromise and/or willful or accidental destruction of information.

D. RESPONSIBILITIES. The Director of the Information Resource Management (IRM) staff will review all software prior to authorization for use on DTSA workstations to insure the procurement/licensing of the software is properly documented and that only licensed commercial or tested public domain software is used on DTSA systems. The IRM Director will also ensure that all DTSA users with access to the Secret DTSA LAN are advised of the procedures as specified in the current Automated Information System Security Plan (AISSP) approved by OSD Physical Security. (Note: The AISSP is a separate reference document and is not attached to this AI).

E. PROCEDURES. The following procedures will be used for installing and operating software on DTSA Delta workstations.

1. No software will be used on or copied onto a DTSA workstation or Server without written approval from the IRM Director or authorized IRM representative.

2. Copyrighted software licensed to DTSA and installed on DTSA equipment shall be installed and used in full compliance with the software copyright.

3. Public domain software or other software which has been tested and accepted by the IRM staff, may be used when this software proves to provide added support to the DTSA mission.

4. DTSA equipment and software shall be used only for official Government business in accordance with DoD Directive 5500.7, subject: Standards of Conduct, page 13,D.3,g as follows: ".... DoD personnel shall not use, directly or indirectly, or allow the use of, any Government property, including property leased to the Government, for other than official purposes."

5. Software loaded onto a classified workstation will not be removed until all security requirements and procedures delineated in the AISSP governing the removal of same have been met. The DTSA Security Manager has authority to inspect the workstations of all DELTA users.

6. All DTSA users will access the approved DTSA software applications through the standard DTSA menu unless a written waiver has been granted by the IRM Director.

7. The IRM staff will provide three catagories of support for DTSA approved software:

a. Fully Supported: IRM will maintain institutional expertise and skills in this software. New versions will be evaluated and purchased as funding becomes available. Users should expect to receive either in-house or commercial training. Examples of this software are WordPerfect 5.1 and WordPerfect Office.

b. Supported to Level of Need: IRM will support this software to the level necessary to support a unique application or requirement. Software of this kind will be issued to individual employees or directorates who maintain their own knowledge base in detailed operation and maintenance. This software will be updated by the IRM staff only when the version change is necessary to the effective operation of the software and/or proves substantially cost effective. Training will be provided when necessary through approved government or commercial courses. Where IRM support is requested, it will be provided on an as available basis and only when in house expertise exists. Examples of this software are ZyIndex and Lotus 1-2-3.

c. Not Directly Supported: This software is provided for use "as is." No warranty other than a best effort IRM evaluation that the software is safe to use and useful for the express purpose stated will be given. No training or technical support will be provided other than that which accompanies the software package. This software will be updated only when it is absolutely necessary or when such updates are freely available to the public. An example of this software is the "List" software.

F. Supplemental Control Procedures. The following procedures will be implemented (and monitored) by the IRM staff:

1. The IRM staff will maintain software license numbers and/or agreements and related purchase documentation for as long as the software is used at DTSA. Licenses for software no longer in use will be transferred in accordance with applicable DoD or FIRMR directives and the software will be deleted from DTSA systems.

2. Each Director within DTSA will be provided a listing of software and hardware for each workstation in his/her Directorate. The IRM staff and each DTSA workstation user will be required to verify the listing of the hardware and software assigned to the users workstation on a semi-annual basis by signing the "ADP Equipment/Software Assignment Form" (see attachment).

3. The IRM staff will conduct random checks of workstations in each Directorate and the Director will be notified in writing should any unauthorized software be detected. Any workstation with unauthorized software cannot be used until a virus scan has been completed by the IRM staff and the unauthorized software is removed.

4. It is the responsibility of the workstation user to promptly notify the IRM staff of any suspected unauthorized changes to the installed software on his/her assigned workstation.

5. DTSA employees who violate these procedures will be subject to disciplinary action.

G. EFFECTIVE DATE. This instruction is effective immediately.

H.P. Ady. III
Director, Resource Management
Defense Technology Security Administration

Attachment
As stated

DTSA ADP EQUIPMENT/SOFTWARE ASSIGNMENT FORM

User Name: _____

Directorate: _____

Date: _____

The ADP equipment/software listed below and in the attachment has been assigned to you. Please verify the information is accurate and report any discrepancies to IRM/DPI.

_____

ADP Equipment

See Attachment 1.

_____

ADP Software

See Attachment 2.

_____

I have verified that the above information is accurate. I understand that no change in the foregoing assigned equipment/software may be made unless authorized in writing by a representative of the Information Resource Management staff of the DTSA Resource Management Directorate. I understand that no software may be copied without such authorization. I understand that a violation of these requirements is subject to disciplinary action.

| | |
|---|---|
| Signature (IRM Representative) | Signature (User) |
| Date | Date |

Attachment(s)
As stated

**AUDIT TEAM MEMBERS**

William F. Thomas, Director, Readiness and Operational Support Directorate
Harrell D. Spoons, Program Director
Marvin L. Peek, Project Manager
John Van Horn, Team Leader
Lisa Earp, Auditor
Rhonda Carter, Auditor
Nancy Cipolla, Editor
Paula Stark, Secretary