

THE DRUG ENFORCEMENT ADMINISTRATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS

EXECUTIVE SUMMARY

Department of Justice (Department) components maintain a large inventory of property, such as weapons and laptop computers, that could result in danger to the public or compromise national security or law enforcement investigations if not properly controlled. In March 2001, the Office of the Inspector General (OIG) audited the Immigration and Naturalization Service's (INS) management of its property and found, among other things, that the INS did not have adequate controls over weapons. In particular, the audit noted that the INS categorized more than 500 weapons as lost, missing, or stolen. After that audit, the Federal Bureau of Investigation (FBI) reported many weapons and laptop computers were missing from its inventory.

In response to concerns about the Department's accountability for its weapons and laptop computers, the Attorney General asked the OIG to conduct audits of the controls over the inventory of such property throughout the Department. The OIG therefore conducted separate audits of the controls over weapons and laptop computers at the FBI, the Drug Enforcement Administration (DEA), the Federal Bureau of Prisons, and the United States Marshals Service.¹ The OIG will issue separate reports on the audits of each of these components, and a capping report describing the results from all the audits. This report covers the audit in the DEA.

The DEA's mission is to enforce the controlled substance laws and regulations of the United States by bringing to the criminal and civil justice system those organizations and principal members of organizations involved in the growth, manufacture, or distribution of controlled substances that are intended for illicit traffic in the United States. At the conclusion of fiscal year 2001, the DEA had a total of 9,209 personnel (4,529 law enforcement) assigned to offices throughout the United States and foreign countries. As of November 2001, the DEA identified an inventory of about 15,000 weapons and 6,000 laptop computers that assist the DEA in performing its law enforcement mission. According to the DEA, of the 6,000 laptop computers in use, only one is authorized to process classified information.

¹ Since we completed an audit of the INS's management of property in March 2001, we did not include the INS in the review of weapons and laptop computers.

Our audit objectives were to review the DEA's: (1) actions taken in response to the identification of lost or stolen weapons and laptop computers; and (2) management controls over these types of equipment. Our audit focused on the period from October 1999 through November 2001.

Our audit revealed significant deficiencies in the DEA's policies and procedures related to weapons and laptop computers. We also found weaknesses in the DEA's management of purchases, receipts and assignments, transfers, returns of property from employees who leave the DEA, physical inventories, and disposals. The results of our audit are as follows.

DEA Weapons

During the 2-year period covered by our audit, 16 weapons were reported by the DEA as lost (2), missing (2), or stolen (12). This represents about one-tenth of one percent of the current weapons inventory. The losses occurred mainly because agents were careless or did not adhere to established policy. Over one-third of these losses occurred when agents left their weapons unattended.

In total, 4 of the 16 weapons have been subsequently recovered by local law enforcement entities. From the information available, we determined there was no apparent direct physical harm to the public caused by the weapons' loss; however, it should be noted that the circumstances surrounding the weapons' recovery were related to possible criminal activity. The weapons were recovered as a result of local law enforcement arrests, searches, and investigations. Two recovered weapons were being held as evidence by law enforcement entities.

We reviewed the policies and procedures followed when the 16 weapons were lost, missing, or stolen. We found that the DEA performed an investigation in all 16 cases. In eight cases, the agent responsible for the loss was suspended from 1 to 30 days. However, our review also found the following deficiencies in DEA practices, which we consider significant because of the potential impact these weapons have on the public if lost, missing, or stolen:

- Three of the 16 weapons had not been entered in the National Crime Information Center (NCIC) computer system by the law

enforcement agencies notified.² The DEA should have reviewed the NCIC to ensure all weapons reported as lost, missing, or stolen were entered, and to determine whether such weapons were recovered.

- The reporting of lost, missing, or stolen weapons to DEA management and Department officials was not always timely or complete. For 11 of the 16 weapon losses, documentation was not completed within the required 48-hour period. Also, the DEA failed to prepare the semiannual Department Theft Report for 1999 and 2000. In addition, the reports covering 2001 did not include all weapons that were lost, missing, or stolen.

We further reviewed the DEA's policies and procedures relating to the control of the approximately 15,000 weapons in use. The DEA recently implemented a new weapons inventory system and just prior to our audit had completed an agency-wide inventory reconciliation. Our review of the new system, which included tests of a sample of 148 weapons, disclosed internal control weaknesses that could cause significant problems with the reliability of the inventory data. We noted the following:

- The financial system was not integrated with the weapons inventory system to ensure the inventory accuracy. Although our sample of 60 purchased weapons showed that all purchased weapons were recorded in the weapons inventory, we recommend that the DEA should institute an automatic interface between the financial system and this system. This would greatly increase the DEA's accountability for all future purchases of weapons by ensuring weapons are recorded and safeguarded from fraud, waste, or abuse.
- The automated system we observed does not provide an audit trail to ensure that all edits made to the weapons inventory are tracked with an automated exception report. As a result, it would be easy to make inventory edits without management's knowledge.
- The accuracy of the weapons inventory depends heavily on the manual submission of property records to the Firearms Training

² The NCIC is a nationwide criminal justice information system maintained by the FBI. This system provides the criminal justice community with immediate access to information such as stolen weapons, missing persons, vehicles, and criminal history records. The DEA relies on local law enforcement entities to input lost, missing, or stolen weapons.

Unit (FTU) in Quantico, Virginia. This condition raises concerns over the timeliness and completeness of the inventory since the DEA is a worldwide organization. During our site visits our tests of a sample of 148 weapons showed that one weapon was assigned on the inventory to an agent who had retired (the weapon was returned) and two weapons were incorrectly assigned. These inconsistencies resulted from the timing delays inherent in this system.

- The duties at the FTU were not adequately segregated. The same FTU individual was able to receive the weapon, verify the completeness of the shipment, and enter the weapon into the inventory database. The lack of segregation of duties causes additional concern when it is combined with the lack of automatic interface between the financial system and this system, as described above. Without the combination of these controls, purchases could go undetected.
- Not all DEA units conducted an annual physical inventory of weapons in accordance with the DEA's Firearms Policy. Two weapons had not been inventoried in 13 years. Also, the weapon inventory duties at the FTU were not adequately segregated. Persons conducting the inventory also had the ability to modify weapon inventory records.
- Employee Clearance Records for separated employees did not include descriptive detail, such as serial numbers, makes, and models, for weapons returned by employees who leave the DEA.
- The DEA does not obtain written confirmation of receipt of weapons that are excessed to other law enforcement agencies.

DEA Laptop Computers

As stated previously, the DEA has over 6,000 laptop computers, of which 5,286 are inventoried in the Fixed Asset Subsystem (FAS) and 848 are inventoried in the Technical Equipment Information System (TEIS). Our audit disclosed that the DEA has significant internal control deficiencies relating to its FAS property inventory, which includes laptop computers. During our fieldwork, the DEA was not able to provide us with a reliable list of lost, missing, and stolen laptop computers covering our audit period on which to base our audit tests. We therefore are unable to report accurately on the number of the DEA's lost, missing, or stolen laptop computers, and

cannot determine if any lost, missing, or stolen DEA laptop computers resulted in a compromise of national security or investigative information. The DEA has since informed us that it has completed a reconciliation of its property inventory and has determined that 229 laptop computers are unaccounted for.

The DEA stated that the inventory in FAS contained a significant amount of unreliable data, and the DEA was performing an agency-wide reconciliation and inventory validation of its property (excluding weapons). According to the DEA, problems with the inventory data occurred after the DEA converted its previous property system, the M-204 system, to the FAS in October 2000. At the conclusion of our fieldwork, the DEA's reconciliation and validation still had not been completed.

As part of our audit, we tested the DEA's policies and procedures related to the control of the laptop computers in use. Of the 110 laptop computers we sampled on-site, we found that 15 had inventory record errors. Errors included incorrectly recorded serial numbers, property descriptions, locations assigned, and individuals having actual custody of the laptop computer. These errors confirmed the unreliability of the FAS inventory data; however, in our judgment, errors of this nature were not caused by the October 2000 system conversion, but rather point to a lack of internal controls and a failure by DEA employees to adhere to established policies and procedures. Our audit also identified the following internal control weaknesses:

- Some DEA units did not have a valid inventory of laptop computers for several years because biennial physical inventories of accountable property were not performed and the Headquarters Property Management Unit did not validate the inventory results. We also noted an instance where physical inventory duties were not segregated. Further, we noted that the manual inventory procedures in place were prone to error and were less efficient than an automated inventory procedure using barcode scanners.
- The financial system was not fully integrated with the FAS to ensure the accuracy of the inventory for laptop computers. When we sampled 74 laptop computers recently purchased, we found one that was not recorded in the inventory. This condition occurred because the system relies mainly on the initiative of the unit's Property Custodial Assistant (PCA) to ensure purchases made are subsequently included into FAS.

- Laptop computers were assigned in the FAS to the PCA instead of the specific individual who had actual custody. Also, property records maintained by some PCAs were inadequate because the tracking of assigned laptop computers was left to the discretion of the PCA.
- Policy was not always followed to ensure that PCAs were notified when new or transferred laptop computers were sent to their location. As a result, the item may not be identified in the division's inventory until the biennial inventory is conducted.
- Hand receipt confirmations on transferred laptop computers were not used systematically throughout the DEA. This condition increases the chance that items would not be traceable to the individuals who had last possession.
- Employee Clearance Records for separating employees did not include sufficient descriptive detail, such as the DEA property code and property description, for laptop computers returned by employees who leave the DEA. As a result, items may not be returned, or may not be identified until after a biennial inventory is conducted.

In this report, we offer several recommendations that we believe will assist the DEA to improve its management of weapons and laptop computers. Generally, the recommendations include: completing the property inventory and providing a valid inventory to all PCAs; developing internal controls, policies, and procedures for the Weapons property system; developing and implementing policies, procedures, and regulations to strengthen system controls and the reporting of losses; integrating the financial system and the property management system; and issuing advisories to responsible employees.

The details of the audit results are contained in the Findings and Recommendations section of the report. Additional information on our audit objectives, scope, and methodology is contained in Appendix I.

THE DRUG ENFORCEMENT ADMINISTRATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
DEA Property Management Systems	1
Prior Reviews	4
Audit Approach	5
FINDINGS AND RECOMMENDATIONS	6
I. ACTIONS TAKEN ON LOST AND STOLEN ITEMS	6
Items Reported	6
Reports and Investigations of Losses	8
Indications of Public Harm.....	12
Conclusion	12
Recommendations.....	13
II. MANAGEMENT CONTROLS	14
Automated Systems	15
Reconciliation to Financial System	17
Purchases	17
Receipt and Assignment.....	19
Transfer of Property	23
Separated Employees	24
Physical Inventories	25
Disposals	27
Conclusion	27
Recommendations.....	28
APPENDIX I - AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY.....	30
APPENDIX II - CIRCUMSTANCES OF WEAPON LOSSES	33
APPENDIX III - ANALYSIS OF LOST, MISSING, AND STOLEN WEAPONS	35
APPENDIX IV - PROPERTY UNIVERSES AND SAMPLES BY TEST, TYPE, AND LOCATION	36
APPENDIX V - SAMPLE DEA-29	38
APPENDIX VI - SAMPLE DEA-17	39

TABLE OF CONTENTS (Continued)

APPENDIX VII - SAMPLE DEA-16	40
APPENDIX VIII - SAMPLE DEA-12	41
APPENDIX IX - SAMPLE DEA-171a.....	42
APPENDIX X - DRUG ENFORCEMENT ADMINISTRATION'S RESPONSE TO THE DRAFT REPORT	43
APPENDIX XI - OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION, ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	49

INTRODUCTION

The Drug Enforcement Administration's (DEA) mission is to enforce the controlled substance laws and regulations of the United States by bringing to the criminal and civil justice system those organizations and principal members of organizations involved in the growth, manufacture, or distribution of controlled substances that are intended for illicit traffic in the United States. At the conclusion of fiscal year 2001, the DEA had a total of 9,209 personnel (4,529 law enforcement) assigned to offices throughout the United States and foreign countries.

As of November 2001, the DEA had an inventory of about 15,000 weapons, which included semi-automatic weapons, shotguns, submachine guns, and rifles. Also during this time period, the DEA had about 6,000 laptop computers, of which 5,286 laptop computers were assigned to non-technical staff,³ and 848 laptop computers were assigned to technical staff. Almost all the laptop computers used by the DEA are used to process information that is considered sensitive. The DEA stated that it has only one laptop computer authorized to process classified information.

DEA Property Management Systems

Office of Management and Budget Circular A-123⁴ requires federal agencies to: (1) establish a management control system that provides reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation; and (2) ensure that transactions are promptly recorded, properly classified, and accounted for in order to prepare timely accounts and reliable financial and other reports. In addition, the Department of Justice Property Management Regulations (JPMR)⁵ requires Department components to issue detailed operating procedures to protect federal property against fraud, waste, and abuse.

DEA guidelines for the general management of laptop computers are contained in its Property Management Handbook. Guidance specifically related to the management of weapons is contained in the DEA Firearms Policy, Section 6122. According to these guidelines, DEA employees are responsible for the proper and reasonable care and safeguarding of property

³ Non-technical staff are employees who perform duties that do not involve the use of specialized laptops for functions such as polygraph analysis and radio programming.

⁴ Management Accountability and Control, dated June 21, 1995.

⁵ Department of Justice Order (DOJ Order) 2400.3, dated August 6, 1998.

assigned to them or located in their work area. An employee whose negligence causes the loss of DEA property, including weapons and laptop computers, may be subject to disciplinary action.

The DEA categorizes weapons and laptop computers as accountable property. The Property Management Handbook classifies accountable property into two categories: non-capitalized and capitalized. Non-capitalized accountable property includes items with an acquisition cost over \$1,000 and under \$25,000. Non-capitalized accountable property also includes weapons, laptop computers, and other sensitive property items such as automated data processing equipment, aviation equipment, laboratory equipment, televisions and VCRs, abandoned/forfeited property, and electronic typewriters. Capitalized accountable property is property with an acquisition cost of \$25,000 or more.

Property Management Personnel

Weapons: The Firearms Training Unit (FTU) located in Quantico, Virginia, is responsible for the overall management of the official weapon property system for all DEA issued weapons. The responsible FTU personnel are the Unit Chief, Chief Armorer, and a secretary. At the DEA's 22 field divisions, there is a designated Primary Firearms Instructor (PFI) assigned to control the weapons inventory.

Laptop Computers: The Property Management Unit (Property Unit), located within DEA headquarters is responsible for the administration of DEA headquarters, domestic offices, and foreign country office accountable property management controls and inventory records.⁶ Its responsibilities include disseminating relevant policies and procedures, coordinating property inventories, and reviewing and approving property management transactions. Responsibilities also include maintaining the automated property system to track the acquisition, movement, and disposal of laptop computers.

The Property Unit is staffed with a Unit Chief, nine Property Management Specialists, and a secretary. Each of the Property Management Specialists is assigned the oversight of specific foreign offices, field division offices, and headquarters offices. They have full access to inventory data for their assigned offices only. For each headquarters unit, division office, district office, resident office, and foreign country office a Property Custodial

⁶ The Property Unit has limited responsibility for management of the weapons inventory; it only certifies the destruction of weapons by DEA.

Assistant (PCA) is designated for property management at his or her respective locations.

Overview of Automated Systems

Weapons: In October 2001, the DEA replaced its automated property management system (M-204 system) with a database system, referred to as the "Weapons Database" by the DEA, to manage its weapons inventory. According to DEA officials, the change was needed because the M-204 system contained a significant amount of unreliable information. In addition, M-204 system users could manipulate data so that items in inventory could be transferred or deleted without approval. To improve controls, the DEA initiated the development of the Weapons Database. According to FTU staff, the DEA performed a physical inventory in FY 2001 and reconciliation of all DEA-owned weapons, completed an official property record for each weapon, and manually inputted the weapons data from each property record into the Weapons Database.

The Weapons Database is inaccessible at DEA field locations. FTU staff use the system to monitor the location and custody of weapons at all DEA locations. Information forwarded by the FTU to field locations is limited to the inventory data for a particular location.

Laptop Computers: The DEA currently has two automated systems that comprise its official property management system for accounting for laptop computers: the Fixed Asset Subsystem (FAS) and the Technical Equipment Inventory System (TEIS). Both the FAS and TEIS systems are used by DEA locations worldwide. The two systems are neither integrated nor reconciled to each other. In October 2000, the DEA converted the automated property management system for laptop computers (the M-204 system) into the FAS.⁷ Following the conversion, the DEA initiated a worldwide, 100 percent physical inventory and reconciliation of accountable property items. Field locations performed the physical inventory and mailed the results to DEA Headquarters. At the time of our audit, the DEA was still performing the reconciliation of the new system. The DEA has since informed us that the reconciliation is complete and that 229 laptop computers are unaccounted for.

⁷ The accuracy of the M-204 system data was not tested by the DEA prior to the conversion, resulting in problems with the reliability of the FAS data. These problems are identified in Finding II.

As noted earlier, each of the nine Property Management Specialists under the supervision of the Chief of the Property Unit is assigned to oversee a group of DEA units. The specialists have full access to FAS inventory data for the groups to which they are assigned, but not for the groups assigned to the other specialists. Also, field locations cannot delete property listed on the FAS, but they can change the status of property – such as “disposed of,” “excessed,” or “transferred.” Field locations cannot access inventory data for other field locations.

The second inventory system for laptop computers, TEIS, is used to track specialized DEA technical equipment worldwide. The inventory recorded on TEIS includes about 800 laptop computers that are used for radio programming, polygraph analysis, or other specialized functions.⁸ The Office of Investigative Technology, located in Lorton, Virginia is responsible for managing the master TEIS database. Two DEA personnel at the Lorton location are designated as “TEIS super users” who can access all TEIS data. Ten other DEA personnel at the Lorton location have limited access to TEIS and a limited ability to modify TEIS data. At DEA field locations, designated personnel in “tech space” also have limited access.

Prior Reviews

The OIG previously audited the DEA’s property management and inventory controls in 1996.⁹ The audit found the DEA had seven separate property systems, each with its own manager and database. Also, there was no property management officer for the overall coordination of the various systems and the audit found that property was not adequately safeguarded against waste or theft. In addition, property record totals were not a reliable indicator concerning the true acquisition value of the DEA’s assets and total property on hand. Each of the recommendations for this audit had been closed. Also, a fiscal year (FY) 2001 financial statement audit¹⁰ revealed that the DEA did not maintain a system that accurately and completely accounted for property and equipment.

⁸ The DEA justification for having the second system is that it provides better controls over specialized items that tend to be checked in and out frequently.

⁹ Office of the Inspector General (OIG) Audit Report 96-10, “DEA Property Management and Inventory Controls.”

¹⁰ Pursuant to the Chief Financial Officers Act of 1990 and the Government Management Reform Act of 1994, audits are required to be performed on the Department’s annual financial statements. These audits are issued by the OIG based on work performed by independent public accountants.

The DEA Inspection Unit performs an inspection of property, including weapons and laptop computers, in domestic field offices every 2 years, DEA Headquarters every 3 years, and foreign offices every 4 years. The inspection includes an evaluation of property management controls, a review of property assignments and physical inventory documents, a physical verification of property, and tests of property records. We examined a sample of recent inspection reports and found that the DEA Inspectors identified findings that pertained to the accountability of laptop computers, such as delays in reporting lost property, items with missing DEA property numbers, inaccurate inventory records, and problems with the inventory reconciliation.

Audit Approach

We obtained from the DEA a listing of weapons identified as lost, missing, or stolen between October 1, 1999 and November 15, 2001. The DEA was unable to provide this information for laptop computers. (See Finding I.) We reviewed the circumstances surrounding each loss and assessed the DEA's reporting and investigative action taken. Further, we looked for indications that the lost property resulted in physical harm to the public. Because the DEA could not provide information on lost, missing, or stolen laptop computers, we could not determine if the lost property resulted in a compromise of national security or investigative information. Our conclusions are presented in Finding I. Appendices II and III contain a summary of our results.

We also reviewed the DEA's management controls over the purchase, receipt and assignment, inventory, and disposal of DEA-issued weapons and laptop computers, as well as the DEA's automated systems. We then assessed the DEA's controls by reviewing property management activities at DEA Headquarters, Justice Training Center, Office of Investigative Technology, Atlanta Division Office, Boston Division Office and San Diego Division Office. At each site, we evaluated relevant property management controls, reviewed documentation practices, and physically inspected property. We also tested, on a sample basis, the accuracy and completeness of the property records. The results of our analyses are presented in Finding II; Appendix IV shows the geographic distribution of the sampled property.

FINDINGS AND RECOMMENDATIONS

I. ACTIONS TAKEN ON LOST AND STOLEN ITEMS

We were unable to test whether the DEA's policies and procedures concerning lost, missing, or stolen laptop computers are adequate because the DEA could not provide us with reliable inventory data. As a result, we could not determine an accurate number of lost, missing, or stolen DEA laptop computers. The DEA was performing an agency-wide reconciliation of its property inventory (excluding weapons), because the inventory, which includes laptop computers, was found by the DEA to be unreliable. We consider this to be a significant internal control weakness, and it is discussed further in Finding II of the report.

During the 2-year period covered by our audit, the DEA reported that 16 DEA weapons were lost, missing, or stolen. Although the number of instances reported is small in relation to the universe, the sensitive nature of these items and the possibility that they can cause public harm heightens the significance of each instance. From the information available, we determined there was no apparent direct physical harm to the public caused by the weapons' loss. The circumstances that led to the reported weapons' status as lost, missing, or stolen included home burglaries, vehicle thefts, and agents leaving their weapons unattended. We also found that the documents required for reporting the losses were not always prepared timely. Some of the losses were not reported to the Department Security Officer, and the semi-annual Department Theft Reports were not prepared for the reporting period covering July 1999 through December 2000.

Items Reported

According to the DEA property management system and information provided by the DEA's Board of Professional Conduct (Board),¹¹ the DEA reports that 2 weapons were lost, 2 were missing, and 12 were stolen during the 2-year period covered by our audit.

We reviewed the circumstances surrounding the loss of each item, actions taken by the DEA to document the loss, the results of follow-up

¹¹ This is an office within DEA that is responsible for determining disciplinary actions and financial liability for lost property.

action taken, and the DEA's compliance with Department and internal regulations. In addition, we looked for any instances in which the loss may have resulted in physical harm to the public.

Our review of the DEA reported 16 lost, missing, and stolen weapons revealed that in 6 instances the losses were due to agents leaving their weapons unattended. These losses are summarized as follows:

- Agent left his weapon on the rear bumper of his vehicle. Reported as lost.
- Agent placed her purse, with her weapon inside, on the floor of a restaurant during dinner. Reported as stolen.
- Agent's carrying pack containing the weapon was stolen as an individual distracted the agent. Reported as stolen.
- Agent left his bag unzipped, with the weapon inside, while practicing at a shooting range. Reported as missing.
- Agent left her purse, with the weapon inside, unattended while attending her son's school function. Reported as stolen.
- Agent left her weapon in a police department gym. Reported as lost.

An additional five losses resulted from home burglaries and four more resulted from vehicle thefts. In some cases, losses attributed to vehicle thefts were due to agents inappropriately leaving weapons in their official government vehicle (OGV).

The remaining loss was discovered during a physical inventory. Although the weapon was listed in the property management system as unaccounted for, property management records indicated the weapon was last assigned to an agent who had resigned. The DEA was in the process of reviewing this weapon.

The losses that resulted from unattended or inappropriate security occurred because of violations of the DEA Firearms Policy, Section 6122.42, Firearms Security, Safety and Storage, which requires all weapons to be stored in a safe place when not being carried. Under this policy, agents are personally responsible for preventing the unauthorized handling or unintentional discharge of all DEA weapons and all authorized personally owned weapons. This policy states that weapons may not be left unattended

or temporarily stored in an OGV, except for the temporary storage of submachine guns or shotguns. Also, agents must place authorized personal weapons, when unattended, in a secure storage area at the agent's office, home, or temporary domicile. To reduce future losses, the DEA should reiterate to its employees the importance of following firearms security, safety, and storage guidelines. The losses and related circumstances are summarized in Appendix II.

Reports and Investigations of Losses

We reviewed documentation related to the weapons losses to determine if: (1) appropriate action was taken by the responsible employee to submit the initial loss report, (2) firearms were promptly entered into the National Crime Information Center (NCIC) computer system, (3) the DEA Board recommended disciplinary actions against the responsible individuals, and (4) items were reported to the Department Security Officer. Our results are detailed below and summarized in Appendix III.

Initial Loss Reports - According to the DEA Firearms Policy, the responsible employee for a weapon is that individual who has custody or control of the weapon at the time of loss, theft, or destruction. Upon discovery of the loss, theft, or destruction of any DEA-issued or approved personally owned weapon, the responsible employee should immediately notify the Special Agent-in-Charge (SAC), Country Attaché (CA), or Headquarters Office Head (HOH). After notification, the aforementioned individuals are responsible for the immediate telephonic reporting of the loss, theft, or destruction to the DEA Headquarters Command Center.¹² Command Center personnel must immediately notify the DEA Office of Professional Responsibility (OPR) and the Board. Subsequent to this, a written notification by the SAC or CA should be given to the OPR, Board, and FTU via Teletype within 48 hours of the discovery of the loss, theft, or destruction of a weapon. Also, within this 48 hour time period, the responsible individual should complete Part 1 of a Liability Assessment Process Form (DEA-29)¹³ and submit it to the local PFI.

The SAC, CA, or HOH then must assign the matter for investigation to a Special Agent of a grade equal to or higher than the grade of the

¹² This is a DEA headquarters unit that serves as a control center for special initiatives and emergency preparedness. It receives information on property losses, shootings, and arrests.

¹³ The DEA-29 is the control document used by DEA to record the results of the investigation and the assessment of responsibility. A sample DEA-29 is displayed at Appendix V.

responsible employee and not directly associated with the responsible employee. The investigation includes verifying the facts and circumstances surrounding the loss, theft or destruction as reported by the responsible employee. The investigation also includes developing additional facts necessary to determine whether the property was being used in an official capacity and if personal negligence contributed to the loss or theft. A completed Report of Investigation (ROI) must be submitted to the Board within 30 days of the loss or theft. The ROI includes a completed DEA-29, police reports, NCIC confirmation reports, and any statements or documents pertinent to the incident.

From our review of available documentation, we found that investigations were initiated on all 16 DEA-reported lost, missing, or stolen weapons according to DEA policy. In addition, DEA-29s were prepared for each of the 16 lost, missing, or stolen weapons. However, we noted that in 11 instances the DEA-29s were untimely. The losses were not reported within the required 48 hours, with delays ranging from 1 day to 89 days. In our judgment, untimely reports delay the initiation of the investigation of the lost or stolen weapon.

NCIC Reports – The NCIC system is the primary nationwide method for tracking stolen and recovered firearms. The DEA Firearms Policy requires the responsible employee to ensure that lost or stolen weapons are entered into the NCIC system within 48 hours through the local law enforcement agency where the loss or theft was reported. If the loss or theft of a weapon occurs at a foreign post, the reporting agent must ensure that the missing weapon is entered into the NCIC through the INTERPOL Command Center of the Treasury Department’s Bureau of Alcohol, Tobacco, and Firearms liaison officer. The reason records of this nature are entered into NCIC through other law enforcement entities is that the DEA only needs to be able to query NCIC for information to support their ongoing investigations.

We examined NCIC records to determine if the DEA reported 16 lost, missing, or stolen weapons were entered into the NCIC system and found that only 10 of the weapons were reported in the NCIC as an “active record,” indicating the weapons had not been recovered. Of the 10 weapons active in the NCIC, we found that one actually had been recovered and placed back in service by the DEA. The record should have been subsequently purged from the NCIC.

Of the six items not in the NCIC as an active record, we found that in three instances the weapons had been recovered and removed as an active

record. Of these three weapons, one had already been placed back in service by the DEA. The other two weapons were recovered by local law enforcement entities and were being held for evidence.

In the remaining three instances, DEA staff reported the losses to the local law enforcement entity; however, the weapons were still not entered into the NCIC. In our judgment, DEA staff should follow-up with the law enforcement entity or check the NCIC, to ensure that the lost, missing, or stolen weapons were subsequently entered.

DEA Board of Professional Conduct (Board) – According to DEA Policy, the SAC or CA must notify the Board in writing within 48 hours after discovery of the loss, theft, or destruction of a weapon. The Board recommends disciplinary actions and financial liabilities, and issues a separate decision letter to the individual responsible for the lost property.

The Board is a permanent, independent office within the DEA, consisting of five members. The members include three Special Agents, one Intelligence Analyst, and one Diversion Investigator.¹⁴ The Board is required to review each investigation report to determine whether disciplinary action is warranted and whether financial liability should be assessed against the responsible individual.¹⁵ After this review, the Board then must send its recommendation to the SAC and the employee. The Board issues a proposal for action to the DEA's Human Resources Division to make the final determination of the action taken. Actions such as warnings, administrative leave, or suspensions are often recommended. In the event of issues involving employee integrity (e.g., driving under the influence, lying during an investigation, or stealing), the DEA OPR should review the case.

We examined the files of the Board to determine if a review was done promptly and an action was taken on the DEA-reported 16 lost, missing, or stolen weapons. In 15 cases, the Board completed its review between 2 to 14 months after the loss report was filed. Because the remaining case

¹⁴ A Diversion Investigator is responsible for investigating cases that involve diverting legal drugs and chemicals used in drug processing for illegal purposes.

¹⁵ The DEA Firearm Policy requires an assessment of individual financial liability to recover the cost of the weapon if the loss or theft of a weapon was caused by an individual's gross negligence. Gross negligence, as defined in the policy, is "a willful, wanton, or reckless disregard for the standard of care required to safeguard the property. It is more than inadvertence, inattention, thoughtlessness, or incompetence, but rather requires the individual be aware of the risk created by his/her conduct, and that the consequence of his/her negligence is substantial."

involved an employee who had left the DEA, the Board made no recommendation. Examples of recommended disciplinary actions taken on 10 cases included suspensions ranging from 1 to 30 days, letters of reprimand, and cautions. In the remaining five cases, the Board did not recommend disciplinary action because it did not find the employee negligent. Appendix II provides more detail regarding the manner of loss and the disciplinary action taken.

Semi-annual Department Theft Report - Department regulations¹⁶ require all components to submit a semiannual Department Theft Report to the Department Security Officer to summarize losses of all personal and government property that occurred during the previous 6 months. The component's Security Programs Manager is required to prepare and submit the reports by January 31 and July 31.

The DEA's submissions to the Department during our 2-year audit period are detailed in the following table.

REPORTING PERIOD	DUE DATE	DATE SUBMITTED
July 1 to December 31, 1999	January 31, 2000	Not submitted
January 1 to June 30, 2000	July 31, 2000	Not submitted
July 1 to December 31, 2000	January 31, 2001	Not submitted
January 1 to June 30, 2001	July 31, 2001	September 05, 2001
July 1 to December 31, 2001	January 31, 2002	January 02, 2002

Source: Department Security Officer

The DEA did not submit any semiannual Department Theft Reports for 1999 and 2000. The individual who was responsible for preparing the reports at the time of our audit said that his predecessor simply had not prepared the required reports. Also, we found that the first semiannual report for 2001 was submitted 36 days late.

We reviewed the lost items identified in the reports for 2001 and compared them to the Board's list of lost and stolen weapons. According to the Board's records, four weapons were reported as being lost, missing, or stolen from January 1 to December 31, 2001. Of the four weapons, we

¹⁶ DOJ Order 2630.2A, Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures, dated October 4, 1977.

found that only one appeared on the semiannual report. The DEA was unable to tell us why the other three were not on the report. The DEA should submit these reports timely to ensure the appropriate Department officials are aware of all items that are lost, missing, or stolen.

Indications of Public Harm

Of the 16 weapons the DEA reported as lost, missing, or stolen, we determined that 4 had been recovered by local law enforcement agencies. To verify whether the loss of these weapons resulted in subsequent harm to the public, we reviewed DEA records and queried the NCIC system and the Treasury Department's Bureau of Alcohol, Tobacco, and Firearms (ATF) National Tracing Center database for any indication that the weapons were used in subsequent illegal activity. The circumstances of the recovery of three of the four lost weapons are summarized below.

- The Baltimore, MD, Police Department recovered one weapon during the arrest of an individual on a handgun violation.
- The Everett, WA, Police Department recovered one weapon during an investigation conducted as a result of a search warrant.
- The Atlanta, GA, Police Department recovered one weapon during a narcotics search at a suspect's residence eight days after it was reported missing.

We were unable to determine the circumstances of the recovery of the remaining weapon because supporting documents did not include details.

Conclusion

We were unable to determine the number of lost, missing, or stolen laptop computers, and whether any losses resulted in a compromise of national security or investigative information. This was because the DEA was unable to provide us with a reliable list of lost, missing, and stolen laptop computers on which to base our audit tests. As discussed in Finding II of the report, the DEA has significant internal control weaknesses and deficiencies relating to the laptop computer inventory.

Regarding lost, missing, and stolen weapons, the DEA reported it had 16 weapons that were in this category during the 2-year period covered by our audit. Four of the 16 weapons have already been recovered by law enforcement entities. Although the number of weapons that were lost,

missing, or stolen is small in relation to the total number of weapons in use by the DEA during the time period, the sensitive nature of these items and the possibility for public harm heighten the significance of each loss. We found that most of the losses were preventable because they resulted from oversight and the failure to follow established DEA policy.

Our audit also found that three weapons reported as missing or stolen were never inputted into the NCIC by local law enforcement entities after the DEA notified them. The DEA reporting of losses to management was also deficient. In some instances, the DEA-29 had been submitted from 1 to 89 days late; the DEA Semi-annual Department Theft Reports were not prepared covering the reporting period July 1, 1999 through December 31, 2000, and the first semiannual report for 2001 was submitted late; and finally, not all losses were reported to the Department Security Officer.

Recommendations

We recommend that the Administrator, DEA:

1. Reiterate to all DEA employees the guidelines for the security, safety, and storage of weapons as outlined in the DEA Firearms Policy, Section 6122.42, Firearms Security, Safety, and Storage.
2. Reiterate to all DEA employees the policy for reporting losses of DEA property as outlined in the DEA Firearms Policy, Section 6122.13, Loss, Theft, or Destruction of a Firearm.
3. Provide semiannual Department Theft Reports for the reporting periods from July 1 to December 31, 1999, and January 1 to December 31, 2000.
4. Ensure the timely and complete submission of future semiannual Department Theft Reports.
5. Ensure that the missing weapons are promptly entered into the NCIC.
6. Ensure that appropriate action is taken on laptop computers that are subsequently determined to be lost, stolen, or missing as a result of the reconciliation of the property inventory.
7. Ensure that a perpetual list of lost, missing, or stolen laptop computers is maintained and that notifications and investigative procedures are performed.

II. MANAGEMENT CONTROLS

We noted significant deficiencies with the DEA's Fixed Asset Subsystem (FAS) property inventory, which controls most of the laptop computers in use by the DEA. These deficiencies are attributed to problems resulting from the DEA's October 2000 conversion to the FAS, failure to follow established policies and procedures, and the lack of integration between the property system and the financial system to ensure all laptop computer purchases are captured in the inventory. In addition, we found the following significant internal control weaknesses: (1) physical inventories were not adequately performed or conducted according to DEA policy; (2) individuals with actual control of the laptop computer were not recorded in FAS; (3) Property Custodial Assistants (PCAs) were not always notified of newly acquired laptop computers; (4) hand receipts were not used systematically throughout the DEA; and (5) clearance records for separated employees contained insufficient detail.

Control weaknesses with the DEA's weapon inventory controls were also present. The database used to track weapons does not provide an adequate audit trail, was not fully integrated with the financial system, and was heavily dependent upon the manual submission of property records to the Firearms Training Unit (FTU). In addition, we found that: (1) weapon purchasing and receiving functions at the FTU were not segregated; (2) physical inventories were not performed annually as required, nor were FTU duties in this area segregated; (3) clearance records for separated employees contained insufficient detail; and (4) confirmations for excessed weapons were not obtained from law enforcement agencies.

We assessed the DEA's compliance with OMB Circular A-123, Federal Property Management Regulations, and Department and DEA policy and guidance. Our review included an evaluation of the controls over weapons and laptop computers at headquarters and four field locations. We obtained background information on the DEA's automated systems and reviewed the DEA's procedures for automated systems, purchases, receipt and assignment, physical inventories, and disposal of accountable weapons and laptop computers. We also tested, on a sample basis, the accuracy and reliability of DEA property records. The universe of weapons and laptop computers assigned to the locations we audited is displayed in Appendix IV,

Table 1. In total, we reviewed 392 items, as summarized in the table that follows and detailed in Appendix IV, Table 2.

TOTAL ITEMS REVIEWED						
	DEA Headquarters	Quantico	Atlanta Field Division	Boston Field Division	San Diego Field Division	TOTALS
WEAPONS	18	96	28	28	38	208
LAPTOP COMPUTERS	53	53	21	22	35	184
TOTALS	71	149	49	50	73	392

Automated Systems

Weapons: The Weapons Database was created by the DEA using off-the-shelf software and is considered by the DEA as its official system to record and manage its weapon inventory. The Weapons Database includes information on each weapon such as the make, model, serial number, custodian, location, acquisition date, cost, and status.

The FTU is responsible for entering new weapons and making changes to the existing Weapons Database, such as the location of the weapon and the agent assigned. The Unit Chief, Chief Armorer, and nine Firearms Instructors of the FTU have access to the main database. The Primary Firearms Instructors (PFI) in field offices do not have access to the main database, but instead are e-mailed a database file that details the weapons recorded for their field division. The PFI is required to make changes to a weapon's status on a DEA-17,¹⁷ Firearms Control Record, and sends the DEA-17 to the FTU for input into the database. According to written guidance from the FTU, DEA-17s may be sent in quarterly.

In FY 2001, the DEA began replacing its automated weapons tracking system, which was part of the M-204 property system, with the Weapons Database. Representatives of the FTU stated that the M-204 system was unreliable and that the new database provided better controls. The Special

¹⁷ A sample of DEA-17 is displayed at Appendix VI.

Agent in Charge (SAC) responsible for the FTU commented that the current database was the best system available for the DEA and meets management needs.

However, the new system employed by the DEA raises concerns over internal controls, segregation of duties, and whether the system is suitable in the long term for an entity with worldwide locations and 15,000 weapons in use. In our judgment, inventory data will not be timely or accurate with the new system. The data entry procedure now in place relies solely on the manual submission of the DEA-17 to the FTU from DEA locations worldwide, and the subsequent input of the information into a database by the FTU staff. To illustrate the present timing problem, we observed that an agent had transferred 6 months prior to our fieldwork; however, the weapon was not assigned to the new field division's weapons inventory. Our review found that the DEA-17 was never submitted, even though DEA Firearms Policy states that agents, upon transfer, are required to provide the gaining office's PFI with their property files within 10 days of reporting to their new office. This error would not have been caught by the DEA until an annual firearms inventory was completed.

We also observed that the new system does not track the edits made to the inventory records contained in the database nor does it provide an automated exception report. This internal control step is necessary to provide management with an audit trail of all edits made, thereby safeguarding the data from unauthorized additions and deletions.

The incorporation of an electronic tracking option for the weapons inventory would offer greater audit trail controls and help eliminate discrepancies in inventory records and provide a source for reviewing the history of a weapon's assignment.

Finally, the DEA does not have a users manual for the Weapons Database. A users manual would provide operators with a reference source and ensure consistency in the implementation of procedures. Other issues that relate to the Weapons Database internal controls and segregation of duties are discussed in later sections of the report.

Laptop Computers: The FAS is used by the DEA for tracking laptop computers that are assigned to DEA staff worldwide. The FAS contains property information such as asset number, serial number, manufacturer, model number, acquisition cost and date, name of PCA, physical location, status, and property condition. The FAS does not, however, identify the specific individual to whom the laptop computer is assigned. By contrast,

TEIS, which is used to track laptop computers assigned to technical staff, does identify the individual to whom the item is assigned.

We were unable to sufficiently test the accuracy and reliability of the FAS inventory as it pertained to the control of laptop computers in use. At the time of our audit, the DEA was having significant problems with the accuracy of the FAS inventory data. According to the DEA, numerous data problems were encountered with its inventory after the October 2000 transfer of data from the M-204 property management system into FAS. The DEA believes the problems resulted from inadequate verification of M204 data prior to the conversion, misclassification of items, discrepancies in location identifiers, and errors in the status of interoffice and intra-office transfers. After encountering this problem, the DEA began an agency-wide property reconciliation. At the completion of our audit fieldwork, the DEA still had not completed its reconciliation. The chief of the Property Unit has since informed us that the reconciliation is complete and 229 laptop computers were determined to be unaccounted for.

Reconciliation to Financial System

According to the Joint Financial Management Improvement Program (JFMIP) Property Management Requirement, the goal of all system interfaces is to facilitate reconciliation between management and financial systems to ensure data accuracy. JFMIP stresses that inventory data entered at a single point of entry should simultaneously populate all databases (financial and management). We determined that the DEA's financial system is not fully integrated with either the Weapons Database or FAS, the systems do not automatically verify the item actually purchased with the item placed into inventory. Instead, the system relies on a manual reconciliation by the PCA at the individual financial transaction level. This control procedure decreases the level of reliability of the data in the two systems, since the reconciliation is based on the initiative of the PCA to investigate what property was purchased. In our judgment, the reconciliation of the property and financial system of weapons and laptop computers should be performed electronically as a single point of entry.

Purchases

Weapons: The procurement of all new weapons is centralized and coordinated by the FTU. The Chief of the FTU is required to complete a DEA-19, Requisition for Equipment, Supplies, or Services, whenever weapons are needed. Then the Special-Agent-In-Charge (SAC) and the Administrative Officer must approve the DEA-19. The approved request is then forwarded

to a contracting officer at DEA headquarters. According to the SAC at the FTU, the request is sometimes accompanied by a cover letter explaining the reason for the purchase. An approved DEA-19 is used as the basis to obligate funds. The Contracting Officer then approves the order and completes the purchase by preparing an order form.

Laptop Computers: Laptop computer purchases are decentralized at the DEA. Offices are allowed to use government credit cards or purchase orders for the acquisitions. The DEA states that whenever laptop computers are purchased at DEA headquarters, a request for laptop computers is submitted; the requesting division submits its request to the Information System Division (SI) for approval. Funds are transferred for the purchase to the SI cost center.¹⁸ Once the request is approved, SI's Acquisition Management Section receives the request and orders the item. Whenever field divisions purchase laptop computers, the requestor prepares a DEA-19 for the approval of the purchase. The Assistant Administrative Officer at the field division requests approval of the purchase from DEA headquarters and then obligates the funds required to make the purchase. The item is then either purchased directly by the cardholder or by the Administrative Officer through a purchase order.

Weapons and Laptop Computers Purchase Sample - We judgmentally selected 60 weapons and 74 laptop computers from vendor invoices to determine if the weapons or laptop computers purchased were recorded in the Weapons Database and the FAS. Details of our sample, by location, are as follows.

ITEMS SELECTED FROM PURCHASE DOCUMENTS						
	DEA Headquarters	Quantico	Atlanta Field Division	Boston Field Division	San Diego Field Division	TOTALS
WEAPONS	0	60	0	0	0	60
LAPTOP COMPUTERS	25	26	4	5	14	74
TOTALS	25	86	4	5	14	134

¹⁸ DEA has designated a series of property accounts in FAS that identify the responsible office, such as each of the domestic and foreign divisions and various Headquarters units.

Our tests revealed that all purchased weapons in our sample had been recorded in the Weapons Database. With the exception of one laptop computer, all purchased laptop computers sampled had been entered into the FAS. We physically located the laptop computer, and as a result of our finding, the PCA entered the item into the FAS. In our judgment, the lack of integration and automated reconciliation between the financial and property systems, which we discussed in the Automated Systems section of this report, contributed to this condition, as did the lack of management oversight to ensure compliance with established DEA policy.¹⁹ Also, failure to record property timely in the official property system timely increases the risk of loss, because theft or misappropriation could go unnoticed.

Receipt and Assignment

Weapons: All weapons purchased are either shipped to the FTU or the Justice Training Center in Quantico, Virginia. According to the Chief Armorer at the FTU, he receives all weapons, counts them, and records their serial numbers on the shipping receipts. Then, the Chief Armorer matches the serial numbers on the weapons to the serial numbers on the packing slip or invoice. Afterwards, the Chief Armorer prepares a handwritten list, by serial number, of weapons received. He then attaches the list to the packing slip as part of the package that is sent to the Administrative Officer for processing the payment. Finally, the packing slip or invoice is stamped to indicate that the weapons are accepted and meet the specifications of the obligating document.

Weapons are entered into the database by the Chief Armorer with a status of "office use"²⁰ until they are received by a designated individual or field division. Once a weapon is issued to an individual at a field division, a DEA-17 is to be completed and forwarded to the FTU. The FTU uses the DEA-17 to update the database with the assigned individual's name.

In our judgment, the duties for receiving and entering weapons into the database are not adequately segregated. The Chief Armorer was the person who not only received the weapon, but also verified the completeness of the shipment and entered the serial number into the database. According to the DEA Chief Financial Officer (CFO) bulletin dated

¹⁹ The DEA Property Management Handbook states that whenever property is received, the PCA should establish a file in which copies of all property-related documents are retained. Within 10 days of the receipt of property, the PCA should affix a DEA property decal to each item, and record the item in FAS.

²⁰ This is the status given to unassigned weapons in the Weapons Database.

June 5, 2001, an individual should not control all aspects of a transaction. Without dividing the key duties of authorization, data entry, and custody of assets, there is a greater risk that error or fraud could occur.

Laptop Computers: Laptop computers purchased by DEA Headquarters are received at the DEA warehouse. Warehouse personnel are responsible for ensuring the purchase is received in good condition and the vendor complied with the specifications of the purchase agreement. Discrepancies are noted on the shipping document and reported to the vendor for resolution. Within 10 days of receipt of accountable property, the PCA at the designated warehouse is required to assign a DEA property number to each item and enter the item in FAS. The warehouse PCA must coordinate with the SI office to arrange for the delivery of the ordered property. Whenever requests are made for a laptop computer by a field division or unit within DEA headquarters, the laptop computer is charged to the respective division or unit cost center and forwarded to the local PCA.

When the field division receives a laptop computer, the local PCA is responsible for obtaining the invoice, packing slip, and receipt if the item was purchased locally with a credit card. Similar to warehouse personnel, the PCA matches these documents to the purchase order. Within 10 days of receipt, the PCA affixes a DEA property number to the property and prepares a DEA-16,²¹ Receipt for Property Card, which lists the purchase order number, the DEA number, and property serial number. The PCA should then enter the property into FAS, and stamp and initial the DEA-16. If DEA headquarters executed the purchase, the local PCA must ensure the laptop computer was already entered into FAS before accepting the laptop computer into the local inventory.

Our review in this area found that the FAS does not list laptop computers by name of the individual assigned, but according to the name of the PCA. Generally, a DEA-12,²² Receipt for Cash or Other Items, is used by the PCA to document the assignment of a laptop computer to an individual. The JPMR states that property custodians are responsible for the day-to-day support of the personal property management program, such as maintaining current records for accountable property within the assigned custodial area. However, we found the DEA policy does not specify how individually assigned property must be tracked. Instead, the tracking method used is left to the discretion of the PCA.

²¹ A sample DEA-16 is displayed at Appendix VII.

²² A sample DEA-12 is displayed at Appendix VIII.

In our judgment, the FAS should include the names of the individuals who have physical custody of the laptop computers for an extended period. This information offers better controls over the accountability of laptop computer assignments. Also, inclusion of this information would reduce the risk of laptop computers being mishandled, lost, or passed from one individual to another without the FAS being updated. Management would have an accurate inventory at any given time without having to research each item in question.

We also found that field division PCAs do not always receive notifications of property transfers that take place within their division. PCAs at two field divisions we visited indicated they sometimes did not receive a copy of purchase orders executed by DEA headquarters on behalf of a sub-office.²³ Under these circumstances, property received at a sub-office might not be entered into the property system until the PCA at the sub-office forward the invoice to the field division PCA. Also, laptop computers assigned to agents during basic agent training at the DEA Justice Training Center remained with the agent after they leave. When these agents reported for duty at their assigned field divisions, they sometimes did not notify the field division PCA they had a laptop computer. In our judgment, the DEA should ensure that PCAs are systematically informed of all new items for which they are held responsible in order to maintain adequate controls of their inventory.

Inventory Testing – To test the accuracy and completeness of the assignment of weapons and laptops computers in the property records, we attempted to physically verify the existence of selected weapons and laptop computers appearing in the Weapons Database and FAS. In addition, we selected a sample of weapons and laptop computers found at each location visited and attempted to reconcile the item to the Weapons Database and FAS. In total, we physically inspected 258 items (148 weapons and 110 laptop computers), as shown in table that follows on the next page. Details of our sample, by property type, location and type of test, appear in Appendix IV, Tables 3 and 4.

²³ DEA field offices and district offices may contain, in addition to the main field office or district office location, several sub-offices and task forces.

ITEMS PHYSICALLY INSPECTED ON-SITE

	DEA Headquarters	Quantico	Atlanta Field Division	Boston Field Division	San Diego Field Division	TOTALS
WEAPONS	18	36	28	28	38	148
LAPTOP COMPUTERS	28	27	17	17	21	110
TOTALS	46	63	45	45	59	258

Of the 148 weapons sampled, we found that one weapon presented to us by an agent was actually assigned in the Weapons Database to another agent. The DEA could not explain the discrepancy. Also, we identified two weapons physically located in an on-site weapon vault that were incorrectly recorded in the inventory records. One weapon was not assigned to the field division's inventory (the weapon was in the Weapon Database) and the other weapon was still shown as belonging to the FTU. We reviewed a copy of the DEA-17 prepared by the field division PFI for both of the weapons and found they were dated August 2, 2001, and August 3, 2001, respectively; however, the inventory had not been updated by the FTU in over three months.

Of the 110 laptop computers sampled, we found that 15 resulted in discrepancies with the inventory data. In seven instances, the serial numbers for the laptop computers did not match the serial numbers associated with the DEA property numbers recorded in the FAS. Also, we were unable to match the serial numbers found on two laptop computers to the FAS because the manufacturer's identification number had been entered instead of the serial number. In addition, two laptop computers did not have DEA numbers. Further, we found that one laptop computer did not appear in the FAS and three laptop computers were not in the possession of the persons assigned on the property card. We found that one of these laptop computers was in the custody of another individual and the other two were located in the work area from which the individuals had transferred. In our judgment, the above discrepancies point to a lack of internal controls and a failure by DEA employees to adhere to established policies and procedures.

Transfer of Property

Weapons: FTU Representatives stated that to track weapons the FTU sends to field divisions, they change the weapon's status in the database to "for issue"²⁴ and assigns the weapon to the receiving field division's inventory. Also, the FTU sends a DEA-12, Receipt for Cash or Other Items, along with the weapon shipment. Upon receipt of the weapons, the field division PFI signs and returns the DEA-12 to the FTU. The PFI also completes a DEA-17 and sends it to the FTU to validate the transfer and identify to whom the weapon is assigned. The FTU uses the DEA-17 to update the Weapons Database. Also, the PFI and agent retain a copy for their records.

Weapons that are transferred between DEA offices are normally sent via Federal Express. The sending PFI notifies the receiving PFI of the transfer by e-mail or telephone, and provides the Federal Express tracking number. The sending PFI prepares a DEA-12, which serves as a packing slip and a temporary custody document. Once the weapon is received, the receiving PFI signs the DEA-12 and sends it back to the sender. Within about 30 days, the receiving PFI is required to send a DEA-17 to the FTU to document the weapon's permanent custody.

As noted earlier in the report, the accuracy of the Weapons Database relies on the timely submission of the DEA-17. Until the DEA-17 is received by the FTU, a weapon that has physically transferred to another DEA office appears on the Weapons Database as being in the custody of the sender. When we performed our inventory testing, as noted above, we found instances where items transferred were not reflected in the inventory timely.

Laptop Computers: DEA officials stated that the use of a DEA-12, DEA-16, or DEA-29 is required for the transfer of all accountable property, which includes laptop computers, made from DEA headquarters to other DEA units. When property is transferred between divisions, there is no similar requirement. The sending PCA is only required to notify the receiver of the transfer via e-mail or telephone.

Within FAS, when items are transferred from DEA headquarters to other units, the item is identified as "pending receipt." When the item is transferred from one division to another, the sending PCA is identified as the custodial officer and that the property is designated as "in transit." After the item is physically present, the receiving PCA is required to enter a "Y" in FAS

²⁴ This is the status given to weapons that are available for issuance upon request.

by the transferred item. At that point, the receiving PCA becomes the custodian of the property.

We observed two weaknesses in this area. The first weakness we observed was that the DEA lacks a strict requirement to use hand receipts for both the transfer of property between field divisions and for the assignment of property within the division. Hand receipts are prepared only at the discretion of the PCA. In our judgment, without the use of hand receipts, controls are inadequate to document who has actual custody of the property. Furthermore, the use of hand receipts would help to resolve conflicts in the event a property transfer is not completed as planned by providing an audit trail (the DEA's policy states that the non-acceptance of transferred assets must be resolved between DEA field divisions).

The second weakness we observed was that DEA Headquarters does not always notify the divisional PCA when a laptop computer is sent directly to individuals in their division. The PCAs at two locations we reviewed, told us they did not realize that laptop computers purchased at DEA headquarters belonged in their divisional inventory until the biennial physical inventory was conducted. In our judgment, DEA headquarters should follow the same procedure of e-mail or telephonic notification that is required of the field divisions when they transfer property.

Separated Employees

DEA guidelines require departing DEA employees to complete an Employee Clearance Record (DEA-171a)²⁵ certifying that all DEA property has been returned. The "Security Activity" section of the form addresses weapons. The "Immediate Supervisor" section addresses personal custody property items, which would include laptop computers. The separating employee must obtain signatures of the responsible officials (e.g., PFIs and PCAs) on the Employee Clearance Record.

Weapons: Although weapons were found to be a category listed on the DEA's Employee Clearance Record, we found that details of the weapon are not included on the form, such as serial numbers or property descriptions. As discussed in Finding I, a weapon that was last assigned to an agent that had resigned was unaccounted for. The agent claimed to the DEA that he had returned the weapon with his other DEA property. We also observed at one location that a retired agent had returned a weapon during the exit process; however, the Weapons Database showed that the weapon was still assigned to the agent. Had the weapon been lost, missing, or

²⁵ A sample DEA-171a is displayed at Appendix IX.

stolen, the retired agent could have been erroneously held accountable. In our judgment, the weapons category on the Employee Clearance Record should be expanded to include more details on the returned weapon. If the location of a weapon is in question, the Employee Clearance Record would show what property had been returned.

Laptop Computers: Similarly, we found that the DEA's Employee Clearance Record did not identify laptop computers as a sign-off item or provide details of what accountable property was retrieved from an employee who leaves the DEA. As noted earlier, the FAS does not include laptop computer assignments by individual, and the tracking of an individual's property assignment is dependent upon the PCA maintaining adequate property records. These conditions increase the need for additional accountability controls and the need to include this information on the clearance record. The TEIS database does list laptop computer assignments by individual; however, we noted one instance in which an employee who left the DEA was still listed as the custodian for a laptop computer that he had returned prior to separation. In our judgment, this was an isolated instance that resulted because the TEIS database was not updated timely. DEA staff located the laptop computer and corrected the TEIS database as a result of our finding. As we noted above regarding weapons, controls over returned laptop computers would be enhanced significantly by including on the Employee Clearance Record what type of personal property was returned, and its DEA property number.

Physical Inventories

Weapons: According to the DEA Firearms Policy, annual physical inventories of all weapons are required. SACs, Lab Directors, and DEA headquarters managers are required to designate an impartial party to inventory weapons and "office use" weapons in each division annually. The policy further states that someone at a higher grade, other than the PFI, should perform the annual inventory.

DEA records showed that not all weapons were physically inventoried in FY 2000. We found as much as 13 years had elapsed since two weapons were inventoried. This occurred because DEA staff did not follow established policy and relied on the physical inventory conducted during an agent's annual firearms qualification. We also found that the system for conducting a physical inventory and inventory reconciliation did not ensure adequate segregation of duties at the FTU. The Unit Chief and secretary of the FTU performed the physical inventory, while the Chief Armorer performed the inventory reconciliation. However, both the Unit Chief and Chief Armorer

were able to modify the Weapons Database. In our judgment, lack of segregation of duties increases the risk of fraud or abuse, and DEA headquarters' current procedures for conducting physical inventories could allow discrepancies to go undetected for years.

Laptop Computers: DEA policy requires biennial physical inventories of accountable property, alternating every other year between DEA headquarters and field divisions. DEA policy also requires that PCAs should not be involved in the physical inventory of accountable property, and staff who perform physical inventories or inventory reconciliation cannot have access to the property management system. Based on our review, we found several deficiencies in this area, as noted below.

First, we noted that the physical inventories were not being conducted biennially as required and were not validated by headquarters. The physical inventory scheduled in 1999 was canceled because of technical problems DEA headquarters had found with the M-204 system; the inventory was postponed until 2000. Because inventories are performed biennially, this situation resulted in a significant period of time where locations did not have a valid inventory. We also found that for two of the three headquarters-level unit inventories we tested, the Property Unit had not validated the reconciliation submitted by the unit PCAs. As a result, the two units did not have a current, valid inventory of laptop computers.

Second, we determined that three individuals who assisted in the most recent physical inventory at one location had the ability to change the data contained in the property management system. The PCA explained that she was unaware of the need to segregate duties and she simply conducted the inventory according to training she said she received.

Finally, the procedures used to take physical inventories of non-TEIS laptop computers were error-prone and more time consuming than necessary.²⁶ We found the Property Unit provided printouts of inventory records to individual DEA units, who performed the physical inventory. Staff at the units took manual counts and made handwritten notations to the printouts to identify discrepancies or furnish explanations. No exception report was prepared. Instead, the DEA unit returned the printouts to the Property Unit, where Property Unit staff make adjustments to the FAS. The Chief of the Property Unit agreed that the current system was outdated and that the use of bar codes and scanners could result in more accurate inventories and take less time.

²⁶ The TEIS Inventories are taken with bar-code scanners, which quickly produce an automated printout of inventory exceptions.

Disposals

Weapons: According to the Chief Armorer, who was responsible for excessing and destroying of DEA firearms, the General Services Administration must provide authorization before a weapon is excessed or destroyed. He explained that weapons that are disposed of are never deleted from the Weapons Database, but are moved to a new location within the database entitled "Destroyed" or "Surplused." Weapons are destroyed by being cut in pieces and melted down. Once the weapons are destroyed, the Chief Armorer notates the database accordingly and files an authorizing letter and other supporting documentation.

Generally, excessed weapons are given to other law enforcement agencies. The procedures for approval, and notation in the database, for excessed weapons are the same as those for destroyed weapons. We found that weapons excessed to law enforcement agencies were supported by proper documentation. However, we noted the DEA did not follow up with law enforcement agencies to ensure that shipped weapons were actually received. If weapons are stolen during shipment, a significant amount of time could elapse before someone at the receiving agency discovers that the weapons from the DEA did not arrive.

Laptops: We did not note any problems with the DEA's procedures for the disposal of laptop computers. A DEA-120, Report of Excess Personal Property, is required to accompany a request for the disposal of laptop computers. The requesting office identifies the laptop computer for disposal and sends the request and DEA-120 to the Property Unit for approval. Prior to authorization for the disposal, the Property Unit receives concurrence from the IS Division as to whether to keep or dispose of the laptop computer. After IS provides the Property Unit with its recommendation, the Property Unit prepares a memorandum with a certification statement,²⁷ which requires the requestor's signature. After the Property Unit approves the disposal, the requesting office disposes of the laptop computer.

Conclusion

General: A problem common to the accountability of both weapons and laptop computers is that the DEA's financial management system is not integrated with the property management systems under review. In our

²⁷ This statement must be signed by the property custodial assistant of the requesting office to indicate that the disposal of the laptop computer was done in accordance with regulations, and all sensitive and classified information have been removed from the laptop computer.

judgment, this condition increases the risk of fraud, waste, and abuse. Another problem common to both systems is that accountability for property retrieved from employees who leave the DEA is weak because the DEA's Employee Clearance Record contains insufficient detail on returned property.

Weapons: The DEA's inventory controls over weapons need improvement because: (1) updated property records were not always submitted timely, (2) duties for receiving weapons and entering them into the Weapons Database were not segregated, (3) duties for conducting inventories and reconciliations were not segregated, (4) a complete inventory of all weapons was not conducted in FY 2000, and (5) follow-up on the disposition of excessed weapons was insufficient.

Laptop Computers: The DEA's inventory controls over laptop computers also need improvement because: (1) conversion of the M-204 system data to the FAS caused errors, making the data unreliable; (2) technical problems with the M-204 system prevented the DEA from performing its 1999 biennial inventory; (3) the FY 2000 inventory was not validated by the Property Unit staff for two of the three headquarters units we tested; (4) the FAS was unable to track laptop computers by individuals assigned; (5) the FAS lacked the ability to automate the physical inventory and produce an exception report; (6) PCAs were not always notified of laptop computer purchases and assignments; and (7) duties for conducting inventories and reconciliations were not segregated.

Recommendations

We recommend that the Administrator, DEA:

8. Develop internal controls, operating manuals, audit trails, and system requirements appropriate to ensure the reliability of inventory data in the Weapons Database.
9. Ensure that a valid inventory is available to all PCAs, based on the completed reconciliation of FAS inventory records to correct the problems created from the conversion from the M-204 system.
10. Integrate the DEA's financial system with the property management systems so that the inventory is routinely and timely updated when a weapon or laptop computer is purchased.
11. Ensure that all purchases are entered timely into the FAS inventory.

12. Ensure that employees who receive shipments of weapons do not have access to the Weapons Database.
13. Record in FAS the names of the individuals who are accountable for laptop computers instead of the names of the PCAs.
14. Ensure PCAs maintain adequate property records to show current assignment of laptop computers.
15. Ensure that field division level PCAs are advised timely by DEA headquarters of purchases and transfers of property items that pertain to their division.
16. Ensure that hand receipts for transfers are used throughout the DEA.
17. Ensure that details such as property descriptions, DEA property numbers, and weapon serial numbers are included on Employee Clearance Records.
18. Ensure that updates to the property system are made timely.
19. Ensure that the physical inventory of weapons is performed annually as required at DEA headquarters.
20. Segregate the duties of staff who take physical inventories, perform reconciliations, and modify the property management system.
21. Ensure that inventories are validated as required for each unit within DEA headquarters.
22. Ensure that confirmations from law enforcement entities are received and forwarded to the FTU when weapons are excessed.