

TABLE OF CONTENTS

| | <u>Page</u> |
|--|--------------------|
| INTRODUCTION | 1 |
| Background..... | 1 |
| Weapons..... | 1 |
| Laptop Computers | 2 |
| Property Management Guidelines | 3 |
| Property Definitions | 4 |
| Property Management Personnel | 4 |
| Automated System | 5 |
| Prior Reviews | 6 |
| Audit Approach..... | 7 |
| FINDINGS AND RECOMMENDATIONS | 9 |
| I. ACTIONS TAKEN ON LOST AND STOLEN ITEMS | 9 |
| Items Reported | 9 |
| Lost or Stolen Weapons | 11 |
| Lost or Stolen "Red Handles" | 16 |
| Lost or Stolen Laptop Computers..... | 17 |
| Reports and Investigations of Losses of Weapons and Laptop Computers..... | 20 |
| Initial Loss Reports..... | 20 |
| NCIC Report..... | 21 |
| Office of Professional Responsibility | 23 |
| Department Semiannual Report | 24 |
| Indications of Public Harm..... | 25 |
| Weapons | 26 |
| Laptop Computers..... | 29 |
| Conclusions..... | 30 |
| Recommendations..... | 31 |
| II. MANAGEMENT CONTROLS | 32 |
| Physical Inventories | 32 |
| Items Tested..... | 34 |
| Purchases | 35 |
| Weapons | 35 |
| Laptop Computers..... | 36 |
| Reconciliation to Financial System | 37 |
| Receipt and Assignment..... | 38 |

| | |
|--|----|
| Weapons | 38 |
| Laptop Computers..... | 38 |
| Armory Weapons | 40 |
| Pooled Laptop Computers | 41 |
| Specialized Equipment and Rapid Mobilization Teams | 41 |
| Separated Employees | 41 |
| Disposals | 44 |
| Weapons | 44 |
| Laptop Computers..... | 45 |
| Conclusions..... | 46 |
| Recommendations..... | 47 |

APPENDICES:

| | |
|---|-----|
| I. – AUDIT OBJECTIVES, SCOPE AND METHODOLOGY | 48 |
| II. – CIRCUMSTANCES OF WEAPON LOSSES | 51 |
| III. – CIRCUMSTANCES OF LAPTOP COMPUTER LOSSES | 60 |
| IV. – ANALYSIS OF LOST AND STOLEN WEAPONS | 81 |
| V. – ANALYSIS OF LOST AND STOLEN LAPTOP COMPUTERS..... | 87 |
| VI. – PROPERTY UNIVERSES AND SAMPLES BY TEST, TYPE, AND LOCATION | 95 |
| VII. – RESULTS OF FBI INVENTORY CONCLUDED MARCH 31, 2002 | 97 |
| VIII. – DETAIL OF MISSING “RED HANDLES” | 100 |
| IX. – COMPUTATION OF MISSING ITEMS..... | 101 |
| X. – ABBREVIATIONS AND FORMS | 102 |
| XI. – AUTHORITIES CITED IN AUDIT REPORT | 104 |
| XII. – FORM FD-500 | 105 |
| XIII. – FORM FD-193 | 106 |
| XIV. – FORM FD-281 | 109 |
| XV. – FORM FD -519..... | 110 |
| XVI. – FORM O-96..... | 111 |
| XVII. – FORM SF-122..... | 112 |
| XVIII.- FORM FD-79 | 113 |
| XIX. – FBI RESPONSE TO THE DRAFT REPORT..... | 114 |
| XX. – OIG ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT..... | 120 |

INTRODUCTION

Background

The FBI, which is the principal investigative arm of the Department of Justice, has investigative jurisdiction over violations of more than 200 categories of federal crimes, including counterterrorism, drugs/organized crime, foreign counterintelligence, violent crimes, and white-collar crimes. The FBI employs approximately 11,000 Special Agents and 15,000 support personnel assigned to FBI Headquarters in Washington, DC; 56 field offices across the United States; the Training Academy at Quantico, VA; and 47 overseas offices.

As of August 2001, the FBI reported an inventory of approximately 50,000 weapons and 15,000 laptop computers to assist its employees in performing their law enforcement mission.

Weapons

Weapons used by the FBI include revolvers,¹ semi-automatic pistols, rifles, carbines, shotguns, tear gas guns, and submachine guns. Within the FBI's property records the term "weapons" includes not only those handguns and shoulder weapons used operationally, but also certain items called "red handles" that are used for training purposes.² In this report, we generally treat functional weapons and "red handles" separately.

¹ On August 20, 2001, the FBI's Firearms Training Unit issued a memorandum directing the recall of all issued revolvers. According to the memorandum, "revolvers cannot be integrated into pistol qualification courses" and, consequently, firearms instructors had to "expend finite training time to run additional qualification courses exclusively for revolver shooters." The memorandum also cited the costs of maintaining spare parts and ammunition for revolvers as reasons for the recall.

² These items include "red handles," which are incapable of firing live ammunition, "blue handles," which can fire only blanks, and "simunition" weapons that can fire only special "paint marking" ammunition. Some "red handles" were originally purchased to fire live ammunition and later converted by FBI gunsmiths, while others were purchased from the manufacturer as "red handles." The FBI's Firearms Training Unit considers it unlikely that anyone would convert a "red handle" back to a functional weapon because the process would be tedious, time-consuming, and far more expensive than the cost of a new weapon. According to the FBI, converting a "red handle" back to a functional weapon would require the services of a skilled gunsmith and the acquisition of parts available only from the manufacturer or a licensed gun dealer.

Laptop Computers

The Department's Security and Emergency Planning Staff (SEPS), an office within the Justice Management Division, maintains records of the number of laptop computers each Department component has authorized for processing classified information. Classified information or national security information (NSI) is information, which if disclosed, could cause harm to the national security or foreign relations of the United States.³ On September 28, 2000, the FBI reported to SEPS that there were 10,003 total laptop computers in the FBI and their security level was as follows: 5 Top Secret; 8,000 Secret; 1,711 unclassified; and 287 miscellaneous (damaged, no hard drive, unusable).⁴

³ Classified National Security Information (NSI) is information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. There are three classification levels of classified NSI. Each level is a measurement of the sensitivity of that information and the damage it could cause to the United States national security if disclosed. These are the only levels authorized for classified NSI:

TOP SECRET – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

SECRET – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

CONFIDENTIAL – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Additionally, there is a category of information known as "Sensitive Compartmented Information" (SCI), or "Codeword," which is afforded more stringent protection because of its extreme sensitivity. Access to SCI is closely controlled and is granted only after a need for such access has been clearly established. (U.S. Department of Justice, Security and Emergency Planning Staff, *Classified National Security Information: Reference Booklet*, June 1998, pp. 1 and 3)

⁴ At the start of our audit in August 2001, approximately 11 months after the report to SEPS, the FBI provided us with data showing a total inventory of 15,077 laptop computers. We relied on this figure during our audit.

FBI policy states that all laptop computers

are authorized to process classified information up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET). The processing of Top Secret and SCI [Sensitive Compartmented Information] information is not authorized on portable microcomputers without written authorization by the FBI's SPM [Security Programs Manager].⁵

It is important to note that classified information is not the only information that needs to be protected from unauthorized disclosure. The *FBI Security Handbook* states in part:

Sensitive information is information that, if disclosed, could adversely affect the ability of the FBI to accomplish its mission. Examples of sensitive information might be the identity of undercover agents, names of people under investigation, tax return information, or personal data on individuals. While not directly affecting the national security of the United States, unauthorized disclosure of sensitive information can endanger people, hamper investigations, misdirect resources, and cause embarrassment. All FBI information is considered sensitive and must be protected from unauthorized disclosure.⁶

Property Management Guidelines

Office of Management and Budget Circular A-123⁷ 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

⁵ The FBI's *Manual of Investigative Operations and Guidelines*, Section 35-9.4.6(4). The FBI uses the term "portable microcomputer" interchangeably with the term "laptop computer."

⁶ *FBI Security Handbook*, page 1.

⁷ *Management Accountability and Control*, dated June 21, 1995.

prepare timely accounts and reliable financial and other reports. The *Justice Property Management Regulations*⁸ require Department components to issue detailed operating procedures to protect federal property against fraud, waste, and abuse.

The FBI guidelines for the general management of property are contained in its:

- *Accountable Property Manual*;
- *Manual of Investigative Operations and Guidelines* (MIOG); and
- *Manual of Administrative Operations and Procedures* (MAOP).

According to these guidelines, FBI employees are responsible for the proper and reasonable care and safeguarding of property assigned to them or located in their work area. An employee whose negligence causes the loss of FBI property may be subject to disciplinary action.

Property Definitions – The FBI’s *Accountable Property Manual* classifies property into three principal categories: capitalized; accountable (or “nonexpendable”); and expendable.

- **Capitalized Property** – All property with an initial acquisition value of \$25,000 or more is capitalized property that must be posted to the general ledger and accounted for on the annual financial statements.
- **Accountable Property** – Property which, because of its value or nature, must be accounted for on an individual basis on the Property Management Application is accountable property. The FBI treats both weapons and laptop computers as accountable (nonexpendable) property.
- **Expendable** – Supplies and equipment which are normally consumed within a one-year period are considered expendable.⁹

Property Management Personnel – According to the *Accountable Property Manual*, the Chief of the Property Procurement and Management

⁸ Department of Justice Order (DOJ Order) 2400.3, dated August 6, 1998.

⁹ *Accountable Property Manual*, Introduction and Section 2, paragraphs 2-4 and 2-22.

Section of the Finance Division is the sole Property Management Officer (PMO) for the FBI. The PMO's duties

include, but are not limited to: the overall administration, coordination, and control of the FBI's Property Management Program; ensuring that adequate systems exist and are documented for accountability of property within the FBI; and to communicate and monitor internal controls of the FBI for maintaining adequate property accountability.

The Special Agent in Charge or the appropriate Assistant Director is the Accountable Property Officer for each field office or Headquarters Unit. The *Accountable Property Manual* states that the responsibilities of these officials

include, but are not limited to: coordinating the property management program within his/her office; providing required leadership and guidance to ensure effective internal control procedures within the office are in compliance with the requirements of the FBI; ensuring property records are created; and ensuring the property management program within their office is in compliance with the FBI's Property Management Program.

To assist them in the performance of their duties, these Accountable Property Officers may designate one or more Property Custodians and/or Supply Technicians, depending on the size and complexity of the office. In addition, the *Accountable Property Manual* states,

*each employee of the Department of Justice who has use of, supervises the use or has control of Government property is responsible for that property. Each employee is obligated to properly care for, handle, use and protect Government property issued to or assigned for the employee's use at or away from the office.*¹⁰

Automated System – The FBI employs the automated Property Management Application (PMA) "to properly and accurately account for all property that the FBI acquires, transfers, and retires."¹¹ The PMA uses a

¹⁰ Section 1, paragraph 1-5.

¹¹ *Accountable Property Manual*, Section 2, Paragraph 2-38.

variety of data fields to identify each item, including a barcode number assigned by the FBI, the serial number, the cost center code for the office where the item is located, a description of the item, and other necessary information. The PMA also records a cost center code (0299) for all items assigned to individual employees rather than an office. Finally, the PMA can generate a "Property Charged Out" report that documents all accountable property assigned to each active and separated employee.

The FBI's Firearms Training Unit (FTU) supplements the PMA with index cards for each weapon in inventory. Like the PMA, the index cards document the serial number, barcode number, initial assignment, and final disposal of weapons, but the index cards also track certain information that PMA was not designed to record. For example, the index cards track the repair history of all weapons.

Prior Reviews

Automated Data Processing General Controls – The OIG audited the FBI's automated data processing general controls in 1990. The audit found that the FBI could not "account for over 2,000 pieces of ADP equipment some of which may contain sensitive data."¹² The OIG recommended that the FBI "locate or reconcile" the ADP equipment in question. In response, the FBI reported that "all FBI organizational entities" had reviewed the "items assigned which were listed on the FBI inventory" as unaccountable property. As of July 23, 1990, the FBI stated that only 74 items, valued at \$188,249, remained unaccounted for. According to the FBI, the discrepancies originally noted by the auditors had resulted from a variety of causes, including duplicate entries in the property system, transposed serial numbers, miscoding of items, erroneously listing surplus items as unaccountable while they were pending disposal, and "rapid deployment of ADP equipment critically needed to support the investigative mission."

FBI Property Management – The OIG previously audited the FBI's management of property in 1992.¹³ That audit found material weaknesses in "the FBI's system of inventory and administrative controls in the property management cycle." The OIG recommended that the FBI "locate and account for all items reported as unaccounted for," reconcile and update the inventory, and take numerous other corrective measures. In response, the FBI reported that it had accounted for 32 of 40 items previously reported as

¹² OIG Audit Report 90-15, *The Federal Bureau of Investigation's Automatic Data Processing General Controls*, dated September 1990.

¹³ OIG Audit Report number 92-13, *Federal Bureau of Investigation Property Management*, dated July 1992.

unaccounted for in one category, and 663 of 799 items previously reported as unaccounted for in another category.

FBI Annual Financial Statement – The Chief Financial Officers Act of 1990, as amended by the Government Management and Reform Act of 1994, requires 24 agencies of the Executive Branch and other agencies designated by the Office of Management and Budget to prepare and have audited organization-wide annual financial statements. The Inspectors General of the various departments are responsible for these audits but they may contract with independent public accountants to conduct them. In their reports for fiscal years 1999, 2000, and 2001, the independent auditors who performed audits of the FBI's financial statements identified material weaknesses in the area of property management. They specifically reported the FBI needs to improve its procedures related to the timely and accurate recording, reconciliation, and reporting of property and equipment in the PMA, the subsidiary record-keeping system that supports amounts reported in the annual financial statements.¹⁴

Audit Approach

We obtained from the FBI a listing dated July 11, 2001, of weapons and laptop computers identified by the FBI as either lost or stolen. We also asked the FBI to inventory all weapons and laptop computers and report the results to us as of September 30, 2001. For various reasons, including the terrorist attacks of September 11, 2001, the FBI was unable to complete this task until much later. The FBI conducted an inventory, in stages, of all accountable property. The inventory of property charged to the various FBI divisions was completed on January 31, 2002, and the inventory of property issued to individual employees was completed on March 31, 2002.¹⁵

Our audit focused on the period from October 1, 1999 through January 31, 2002. During this period, the FBI reported property losses of 212 weapons, 142 "red handles," and 317 laptop computers.¹⁶ Although our

¹⁴ OIG Audit Report 00-15, *Federal Bureau of Investigation Annual Financial Statement, Fiscal Year 1999*, dated July 2000, and OIG Audit Report 01-14, *Federal Bureau of Investigation Annual Financial Statement, Fiscal Year 2000*, dated May 2001. The financial statement audit report for FY 2001 has not been issued yet, but the auditors found similar weaknesses in that year as well.

¹⁵ See Appendix VII for a summary of the results as of March 31, 2002 as they relate to weapons and laptop computers. In this report, we take note of the March 31, 2002 results, but we did not audit them because our fieldwork was completed before that date.

¹⁶ See Appendix IX for the process by which we arrived at those figures.

audit focused principally on those losses, we also reviewed certain losses that occurred outside this period to gain an understanding of the magnitude of the conditions noted in this report. We reviewed the circumstances surrounding each loss and assessed the FBI's actions to report and investigate those losses. Further, we looked for indications that the lost property resulted in physical harm to the public or compromised national security or investigative information. Our conclusions from the above analyses are presented in Finding I, and Appendices II and III contain a summary of our results.

We also reviewed the FBI's management controls over the purchase, receipt and assignment, inventory, and disposal of FBI-issued laptop computers and weapons. We assessed these controls by reviewing property management activities at FBI Headquarters and four selected field locations.¹⁷ At each site we: (1) evaluated relevant property management controls; (2) reviewed documentation practices; and (3) physically inspected property. We also tested, on a sample basis, the accuracy and completeness of the property records. The results of the above analyses are presented in Finding II; Appendix VI shows the geographic distribution of the sampled property.

¹⁷ We judgmentally selected Denver, CO; Jacksonville, FL; Los Angeles, CA; and, New Haven, CT, to include large, medium, and small offices and to achieve a geographical distribution.

FINDINGS AND RECOMMENDATIONS

I. ACTIONS TAKEN ON LOST AND STOLEN ITEMS

FBI data show that between October 1, 1999 and January 31, 2002, a total of 212 functional weapons, 142 "red handle" training weapons, and 317 laptop computers were reported as either lost or stolen. We determined that in several instances missing FBI weapons were subsequently used in the commission of a crime or were recovered at the scene of a crime. In many instances, the loss of weapons and/or laptop computers was preventable because it resulted from carelessness on the part of individual employees or failure to adhere to FBI policies.

In this section of the report, we examine the FBI's actions taken on lost and stolen items. Our discussion focuses on the following topics: Items Reported; Reports and Investigations of Losses; and Indications of Public Harm.

Items Reported

As of August 2001, the FBI reported that it had approximately 50,000 weapons and 15,000 laptop computers. However, significant numbers of both items were known to be missing.

The following table displays the numbers of missing items as of four dates mentioned in this report: July 11, 2001; January 31, 2002; March 31, 2002; and the period from October 1, 1999 through January 31, 2002.

| Lost or Stolen Items | | | | |
|-------------------------|----------------|----------|----------|-------------------|
| | FBI Data As Of | | | OIG Audit Period |
| | 07/11/01 | 01/31/02 | 03/31/02 | 10/01/99-01/31/02 |
| Weapons | 351 | 399 | 423 | 212 |
| "Red Handles" | 94 | 161 | 158 | 142 |
| Laptop Computers | 184 | 366 | 310 | 317 |

The figures for July 11, 2001, were untested data provided to us by the FBI early in our audit. The figures for January 31, 2002, and March 31, 2002, resulted from a physical inventory conducted by the FBI in stages.

We focused our audit initially on the period from October 1, 1999 through September 30, 2001, for conformity with our audits of the USMS, DEA, and BOP. However, we expanded the review period through January 31, 2002, so that we could utilize the results of the FBI inventory concluded on that date of property charged to its various divisions.

We determined that the FBI reported the loss or theft of 212 functional weapons, 142 "red handle" training weapons, and 317 laptop computers between October 1, 1999, and January 31, 2002. We made this determination by reconciling data provided to us by the FBI as of July 11, 2001, and January 31, 2002, and eliminating losses or thefts that occurred outside our review period.¹⁸

We estimate the replacement cost of these lost and stolen items would be \$68,649 for the functional weapons, \$3,834 for the "red handles," and \$1,008,302 for the laptop computers.

The 212 missing functional weapons equate to less than one-half of one percent of the inventory of approximately 50,000 weapons, while the 317 missing laptop computers represent 2 percent of the approximately 15,000 in inventory. Nevertheless, the potential harm resulting from the loss of weapons or laptop computers makes these losses significant.

The following table provides a more detailed breakdown of the missing items that we reviewed. It is based on lists of missing property reported by the FBI as of July 11, 2001, and January 31, 2002.

¹⁸ See Appendix IX for our computation of these figures.

| MISSING ITEMS 10/01/99 – 01/31/02 | | | |
|--|-------------|---------------|-------------------|
| PROPERTY TYPE | LOST | STOLEN | TOTAL |
| WEAPONS | 107 | 105 | 212 ¹⁹ |
| “RED HANDLES” | 142 | 0 | 142 ²⁰ |
| LAPTOP COMPUTERS | 300 | 17 | 317 ²¹ |
| TOTAL | 549 | 122 | 671 |

Source: FBI Finance Division, Property Procurement and Management Section

We reviewed the circumstances surrounding these losses and the actions taken by the FBI to document and follow up on each, including compliance with Department and internal regulations. In addition, we looked for indications that the losses resulted in physical harm to the public.

Lost or Stolen Weapons

The following table summarizes the circumstances surrounding the 212 weapons reported lost or stolen between October 1, 1999 and January 31, 2002.

¹⁹ After the conclusion of our fieldwork, the FBI reported to us that five lost and three stolen weapons had been found.

²⁰ After the conclusion of our fieldwork, the FBI reported to us that nine missing “red handles” had been found.

²¹ FBI data show 27 of the 317 laptop computers were located, including 26 located after the audit review period.

| Summary of Missing Weapons | |
|------------------------------------|------------|
| Stolen from FBI Vehicle | 40 |
| Stolen from Employee Residence | 18 |
| Stolen from POV ²² | 12 |
| Miscellaneous Thefts ²³ | 35 |
| Stolen | 105 |
| Unexplained Losses | 76 |
| Presumed Destroyed | 9 |
| Miscellaneous Losses ²⁴ | 22 |
| Lost | 107 |
| Total | 212 |

Source: OIG Analysis of FBI Reports of Lost/Stolen Weapons

As shown above, 70 of the 212 losses (33 percent) involved thefts from FBI vehicles, private vehicles, or employee residences. Although our review of FBI files found instances where such thefts occurred despite reasonable precautions by the FBI employee, we also found numerous losses of weapons that resulted from carelessness or failure to adhere to FBI policy.

The following are some of the egregious examples identified from the universe of lost or stolen weapons.²⁵

Avoidable Losses of Weapons

- A shotgun was stolen from an FBI vehicle parked overnight in a Special Agent's driveway. The Special Agent failed to activate the car alarm because it had sounded erroneously on several recent occasions during the night. The theft occurred on July 15, 1992, but was not reported until November 2001. OPR opened a case on February 2, 2002, which was still pending at the end of our fieldwork. (See Appendix II, item 202.)

²² Privately owned vehicle.

²³ These weapons were stolen under a variety of circumstances. For example, one weapon was stolen from a rental car. Another was stolen from a Special Agent's checked luggage on an aircraft.

²⁴ These weapons were lost under a variety of circumstances. For example, a weapon assigned to a Special Agent who was killed in the line of duty could not be located.

²⁵ Some of these losses occurred outside the audit period.

- A shotgun and a submachine gun were stolen from an FBI vehicle parked on the street in New York. A Special Agent parked the car at about 2:00 pm on December 26, 2001, and discovered the break-in when returning to the car at about 6:00 am the following day. The submachine gun and the shotgun were taken from a rack mounted on the front seat of the vehicle. OPR opened a case on February 21, 2002, which was still open at the end of our fieldwork. These weapons were not among the 212 we reviewed.
- While attending a high school football game, a Special Agent left a handgun under the driver's seat of a vehicle. When the Special Agent returned two hours later the weapon was missing. This theft occurred on November 5, 1999 and OPR opened a case on November 29, 1999. This was the second loss/theft of a weapon involving this Special Agent, and resulted in a three-day suspension without pay. (See Appendix II, item 16.)
- A Special Agent placed a backpack containing an FBI issued handgun on the ground next to an FBI vehicle. The Special Agent then drove off, leaving the backpack behind. The loss occurred on June 18, 2001. OPR opened a case on July 24, 2001 and the Special Agent received a Letter of Censure on February 20, 2002 (See Appendix II, item 139).
- A Special Agent left an issued handgun in a public telephone booth on October 25, 1998. The matter was referred to the FBI's OPR. The Special Agent received a Letter of Censure on December 9, 1998. The Form FD-500 reporting the loss to the FTU was dated September 29, 2000 (See Appendix II, item 62).
- A Special Agent left a fanny pack containing an FBI issued handgun on the back seat of a taxicab on April 8, 2001. OPR opened a case on May 25, 2001. The Special Agent was issued a Letter of Censure on December 17, 2001 (See Appendix II, item 134).

FBI Policy Regarding Storage of Weapons

The losses described above could have been avoided if the employees in question had adhered more closely to FBI policies. The MIOG states FBI policy for the storage of weapons in FBI offices, at employee residences, and in motor vehicles.

In FBI Space

- In the office, *handguns may be retained in a locked desk drawer or in a locked briefcase provided the briefcase is stored in a vault, wardrobe cabinet, cabinet drawer or other secure place designated by the SAC [Special Agent in Charge].*²⁶

At Residences

- *When devices or containers are provided by the Bureau for the storage of weapons away from Bureau space, SAs [Special Agents] should make use of this equipment whenever possible.*²⁷
- *When unattended, each firearm must be made inoperable by one or more of the following methods: (a) Remove and separate the source of ammunition. (b) Install commercially available pistol lock, trigger lock, cable lock, or other device which will prevent the weapon from being fired. (c) Contain in a commercially available lock box or other container which will provide appropriate security.*²⁸
- The MIOG also cautions Special Agents to ensure the security and storage of their firearm(s) complies with pertinent state and local laws because such laws often provide *severe criminal and civil penalties when anyone is injured or killed as a result of a child obtaining access to a firearm.*²⁹

In Vehicles

- *Firearms may not be left in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use unless the vehicle doors are locked and the firearm is secured in a locked vehicle weapons mount or other secure device or container which cannot be readily removed from the vehicle, and circumstances prevent more secure storage.*

²⁶ MIOG, Part 2, Section 12-6, paragraphs (4) and (6).

²⁷ MIOG, Part 2, Section 12-6.1, paragraph (2).

²⁸ MIOG, Part 2, Section 12-6.1, paragraph (3).

²⁹ MIOG, Part 2, Section 12-6.1, paragraph (4).

- *Firearms may only be stored in vehicle trunks that are alarmed or secured with a case hardened chain and padlock. Even when properly secured, firearms should not be left in unattended vehicles overnight unless required by operational circumstances.*
- *Weapons may be stored in SA's [Special Agent's] personal vehicle only for short periods of time and must be retained in the locked trunk.*
- *Vehicles without trunks are not considered secure storage areas. Specialty vehicles (i.e., vans, pickup trucks) may be equipped with a permanently mounted lock box for temporary weapon storage.*
- *The trunk of a vehicle equipped with a trunk release located in the passenger compartment is not a secure area unless the release can be bypassed or the trunk is alarmed or secured with a case hardened chain and padlock.*

The MIOG also states,

The standards set forth above are MINIMUM standards. Employees are expected to exercise good judgment in providing adequate security to nonexpendable equipment and firearms. Personal inconvenience is not considered an adequate reason for deviation from these minimum standards.³⁰

We believe the FBI can minimize the risk of future losses of weapons by strengthening its current policy.

- The FBI should enhance its policy regarding the storage of weapons at employee residences. Unattended weapons left at a Special Agent's residence should be stored in a commercially available locked container. Separating the source of ammunition and installing a pistol lock are sound practices, but by themselves they will not prevent theft of a weapon left in an open area.
- The FBI should also enhance its policy regarding the storage of weapons in vehicles. Current policy allows for storage of weapons in vehicle trunks that are alarmed or equipped with a case hardened chain and padlock. In our judgment, the FBI should require both measures. It is not sufficient to rely on a car alarm because car alarms are often ignored.

³⁰ MIOG, Part 2, Section 12-6.2, paragraphs (1), (2), (5), (6), (7), and (9).

Types of Missing Weapons

The missing weapons represented the full spectrum of firearms used by the FBI, including handguns, rifles, shotguns, and submachine guns. However, pistols and revolvers accounted for 149 (70 percent) of the lost or stolen weapons. The following table displays the numbers and types of missing weapons.

| MISSING WEAPONS | |
|------------------------|-------------------------|
| TYPE | NUMBER |
| Pistols | 85 |
| Revolvers | 64 |
| Shotguns | 42 |
| Submachine Guns | 10 |
| Derringers | 5 |
| Rifles | 4 |
| Miscellaneous | 1 |
| Unable To Determine | 1 |
| TOTAL | 212³¹ |

Source: OIG Analysis of FBI Data

Lost or Stolen "Red Handles"

A document prepared by the FTU states, "Historically many Agents did not consider 'training' weapons to be 'real' and, consequently, did not afford them the same levels of security they would live fire weapons." A lack of concern about security for "red handles" could certainly result in an environment where those items can be easily misplaced. We recognize that the loss of functional weapons poses a greater risk of harm to the public than the loss of "red handles." Nevertheless, "red handles" are accountable items and could potentially be used in furtherance of a crime.

Our analysis of FBI records found that the 142 missing "red handles" included 109 revolvers, 11 paint guns, 10 semi-automatic pistols, 8 "blue grips," 3 shotguns, and 1 submachine gun. (See Appendix VIII for additional details.) The following photographs show what certain "red handles" look like.

³¹ After the conclusion of our fieldwork, the FBI reported to us that three pistols, three revolvers, one shotgun, and one submachine gun had been found.

"Red Handles"



Lost or Stolen Laptop Computers

We reviewed the circumstances surrounding the losses of laptop computers and the actions taken by the FBI to document and follow up on each, including compliance with Department and internal regulations. In addition, we looked for indications that the losses resulted in the compromise of classified or sensitive information. The following table summarizes the circumstances surrounding the 317 laptop computers lost or stolen between October 1, 1999, and January 31, 2002.

| <i>FBI Missing Laptop Computers Summary</i> | |
|---|---------------|
| Description | Number |
| Unable to Locate | 224 |
| Located After Audit Period | 27 |
| Reported Lost/Stolen While Assigned to FBI Employee | 31 |
| Possible Undocumented Destruction | 9 |
| Possible Undocumented Transfer | 21 |
| No Documentation Provided | 5 |
| TOTAL | 317 |

Source: OIG Analysis of FBI Data

As shown above, 224 laptop computers (71 percent) fell into the category "Unable to locate." We find this particularly disturbing because it means that the FBI simply cannot determine where those laptop computers are, and whether they were lost or stolen.³²

We found numerous losses of laptop computers that resulted from carelessness or failure to observe FBI policy. The following are some examples identified from the universe of lost or stolen laptop computers. The FBI identified the security classification of all but one of the missing laptop computers as "unclassified." The status of the laptop computer listed as item 297 in Appendix III was reported by the FBI as "unknown."

Losses of Laptop Computers

- A laptop computer was stolen from the FBI employee's privately owned vehicle while it was parked at a restaurant where the employee was eating on July 2, 1999. The laptop computer was concealed on the floor on the passenger side of the vehicle. As a result of this theft, the employee received an oral reprimand from the Special Agent in Charge (See Appendix III, Item 20).
- A laptop computer assigned to a Special Agent was stolen from the Special Agent's FBI vehicle on January 31, 2001, while it was parked at the Special Agent's residence. No OPR file was located and no disciplinary action was identified (See Appendix III, Item 94).
- A laptop computer that could not be located at the Washington Field Office had not been seen for at least one and one-half years prior to being reported lost on January 18, 2000. No OPR file was located and no disciplinary action was identified (See Appendix III, Item 225).
- A laptop computer assigned to a Special Agent was stolen during the weekend of May 26 through May 28, 2000, while the Special Agent was traveling on vacation. The exact time and location of the theft could not be determined. An OPR review was opened on December 5, 2000. The review resulted in the Special Agent receiving a Letter of Censure dated September 20, 2001 (See Appendix III, Item 275).
- An assigned laptop computer could not be located in the Special Agent's vehicle on June 13, 2000. The Special Agent last saw the

³² In this report, we are treating these laptop computers as lost because we found no evidence that they were stolen. However, we cannot rule out the possibility that at least some were actually stolen.

laptop computer on June 5, 2000, when it was stored hidden from view under the vehicle's rear seat. The loss was reported in an Electronic Communication dated July 21, 2000. OPR opened a review on November 1, 2000. The Special Agent received a Letter of Censure dated April 16, 2001 (See Appendix III, Item 192).

- A laptop computer was stolen from a Special Agent's vehicle between July 19 and July 22, 2000, while the vehicle was parked in front of the Special Agent's residence. The Special Agent first noticed the loss about August 21, 2000. OPR opened a review on October 11, 2000. The review resulted in the suspension of the Special Agent without pay for three calendar days (See Appendix III, Item 237).
- Two laptop computers were lost while FBI employees were overseas on Government business. In January 2002, a Language Specialist briefly left a laptop computer unattended in a hotel cafeteria in Madrid, Spain, and it was stolen. (The FBI reported the security classification of this laptop computer as "unknown." A Special Agent's assigned laptop computer was stolen from hotel staff in Tokyo, Japan, immediately prior to the Special Agent's departure in November 2001. OPR reviews are pending in both cases (See Appendix III, Items 297 and 298).

FBI Policy Regarding Safeguarding of Laptop Computers

We believe that the losses described above could have been avoided if the Special Agents in question had adhered more closely to FBI policies as articulated in the following citations.

Portable microcomputers (e.g., laptops, notebooks) . . . require extra attention due to the vulnerability that their portability creates.

To the extent possible, portable microcomputers should be kept in the possession of the individual to whom they are issued or charged out.

Like classified documents, portable microcomputers used to process classified information must be secured in locked storage when not under direct personal control. Portable microcomputers should be kept in the possession of the individual to whom they were issued or charged out. Removable hard drives must always remain in the direct personal control of the individual to whom they are issued or maintained in a

secured locked container within FBI-controlled space. The hard drive cannot be left unattended.

*NEVER leave the laptop unattended while overseas.*³³

Reports and Investigations of Losses of Weapons and Laptop Computers

We reviewed the documentation related to the property 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 NCIC; (3) the FBI's OPR performed timely investigations to resolve the incidents; and (4) items were reported to the Department Security Officer. Our results are detailed in Appendices IV and V and summarized below.

Initial Loss Reports

Weapons

FBI policy states, "Reports of lost/stolen firearms-related Bureau property should be submitted to the Firearms Training Unit AND the Adjudication Unit, Office of Professional Responsibility [OPR], for replacement and possible administrative action."³⁴ The FBI uses a "Report of Lost or Stolen Property" (Form FD-500) to report the loss or theft of property (see Appendix XII). However, no time frames are specified for submission of these reports or for the FTU or the OPR to act on reports of missing weapons.

In addition, our review of the Form FD-500 identified shortcomings in the form itself.

- The form has a "date" block for recording the date when it was prepared, but not a "date of loss/theft" block.
- The form has boxes to check if the missing item has/has not been entered into NCIC, but no place to record the date of an NCIC entry or the resulting NCIC number.
- The form has a place to record the name of the individual to whom the property was last assigned/charged out. However, it does not

³³ MIOG, Part 2, Section 35-9.4.6, paragraphs (1), (3), (4), and (6)(b).

³⁴ MIOG, Part 2, Section 12-6.2 (9).

have a comparable place to affix responsibility for pooled property, such as unassigned weapons maintained in the armory.

An August 2001 memorandum from the FTU disclosed “many weapons reported missing at the field office level as far back as the 1970s and 1980s which were not reported to FBIHQ until 2000.” The FTU document also stated, “Absent a rigidly enforced policy to *immediately* report the loss or theft of accountable property, individuals and field offices may not report missing firearms in the hope that the weapons would eventually be located.”

We reviewed the reporting of lost or stolen weapons to FBI Headquarters and found significant deficiencies.

- Because the FBI files lacked sufficient detail, we could not determine how much time elapsed between the loss of 129 weapons (61 percent of the 212 missing weapons) and the date when a Form FD-500 was prepared.
- We determined the elapsed time for reporting 83 of the 212 losses of weapons. The range for preparation of a Form FD-500 was from the same day to 23 years. Only seven of the Forms FD-500 were prepared within five days of the loss of a weapon.

Laptop Computers

Prior to March 9, 2001, FBI policy did not require the routine reporting of lost or stolen laptop computers to OPR. We determined that the loss or theft of only ten laptop computers had been reviewed by OPR.

On March 9, 2001, the Director of the FBI issued a *Memorandum to All Employees* entitled “Portable Microcomputer Security Policy.” This document reiterated various provisions of the MIOG and added a requirement to report all losses of laptop computers to OPR “without exception” because “the loss of a laptop with classified or sensitive information could be potentially more damaging to the FBI than a lost weapon.”

NCIC Report

The NCIC system is generally regarded by law enforcement agencies as the primary nationwide method for tracking stolen or recovered firearms. Therefore, data regarding lost or stolen weapons should be promptly entered into NCIC.

The FBI's policy on entering data into NCIC states,

If government property is lost or stolen, it should be reported immediately by original and one copy of an electronic communication to the Property Procurement and Management Section, Finance Division, FBIHQ, and all uniquely serialized government property reported stolen must be placed in the National Crime Information Center (NCIC). In addition, local authorities should also be notified if concurrent jurisdiction exists.³⁵

In our judgment a deadline of "immediately" is open to interpretation. The FBI should define specific deadlines, such as "within two working days," for reporting lost or stolen weapons and for making NCIC entries.

We queried NCIC on the status of 276 missing weapons³⁶ to determine whether they had been entered into the database and identified 14 weapons for which NCIC had no record. We made this determination after querying both the active and purged NCIC records and failing to locate a record of the weapons in question. Four of the 14 weapons had serial numbers that were found in NCIC; however, the make and model were different from the weapons we were testing. Also, 6 of the 14 "weapons" were "red handles" (noted # in the table below).

³⁵ MAOP, Part 2, Section 6-7.5 (1).

³⁶ We judgmentally selected 276 weapons from a list of 445 that the FBI identified as missing prior to initiating an inventory of its accountable property in June 2001. The 276 weapons were all the weapons the FBI identified as having a "disposition date" after September 30, 1999. The FBI defines "disposition date" as the date when property is removed from its "accountability records."

| WEAPONS NOT IN NCIC | | | | |
|----------------------------|----------------|-------------|--------------|---------------|
| # | BARCODE | MAKE | MODEL | STATUS |
| 1 | F0176217 | Walther | PPK/S | Stolen |
| 2 | F0452224 | S&W | 10-8# | Lost |
| 3 | F0429494 | Colt | OP# | Lost |
| 4 | F0281940 | Raven Arms | MP25# | Lost |
| 5 | F1091534 | S&W | 13 | Stolen |
| 6 | F0482991 | S&W | 13 | Stolen |
| 7 | F0795966 | Sig Sauer | P228 Auto# | Lost |
| 8 | F0019853 | S&W | MP# | Lost |
| 9 | F0019784 | S&W | MP# | Lost |
| 10 | F1224330 | Glock | 22 Auto | Stolen |
| 11 | F0862511 | Glock | 22 Auto | Stolen |
| 12 | F0280565 | Sig Sauer | P226 Auto | Lost |
| 13 | 00305195 | Remington | 870 | Stolen |
| 14 | F0760593 | S&W | 1076 Auto | Stolen |

Source: OIG query of NCIC active and purged records.

Office of Professional Responsibility

Departmental policy allows the Bureaus to establish a Board of Survey or to employ "alternative investigative mechanisms, such as a review by the Office of the Inspector General, Office of Professional Responsibility or internal review" to investigate "the loss, theft, damage, destruction, or other circumstances adversely affecting personal property." Reviews by Boards of Survey or alternative mechanisms must extend to "a comprehensive review and a specific finding of responsibility or no responsibility and may be used as the basis to relieve personal accountability, assess pecuniary liability, and/or disciplinary action referral, as appropriate."³⁷

We determined the FBI had not employed Boards of Survey to carry out the responsibilities mentioned above. Instead, the FBI's OPR was assigned the responsibility to investigate and adjudicate matters involving loss or theft of accountable property. However, OPR advised us that prior to 1997 the Special Agents in Charge handled most missing property cases locally. Consequently, the OPR database of missing property cases relates principally to losses or thefts that occurred since 1997.

³⁷ DOJ Order 2400.3, *Justice Property Management Regulations*, dated August 6, 1998, subparts 128-51.101 (b) and 128-51.102 (a).

Our audit found evidence that only 71 of the 212 losses of weapons (34 percent) were reported to OPR. OPR could not provide us documentation of the remaining 141 losses, so we are unable to determine whether they were, in fact, ever referred to OPR.³⁸ (See Appendix IV.)

As a result of the 71 referrals, the FBI took the following actions:

- 25 Letters of Censure
- 1 Three-day suspension
- 3 Five-day suspensions
- 1 Seven-day suspension
- 1 Six-months' probation.

In addition, nine referrals were still pending when we completed our fieldwork. In 31 instances, OPR determined the employee in question took reasonable precautions to secure the weapons and no disciplinary action was warranted.

Department Semiannual Report

Department regulations require all components to submit semiannual reports (due January 31 and July 31) to the Department Security Officer "summarizing thefts that have occurred within their respective organizations during the preceding six months. The report shall include the results of investigations, corrective measures that were instituted to prevent repetition and any special security problems that should be brought to the attention of the Department Security Officer."³⁹

The Departmental order applies to any theft of government property and does not differentiate by types of property. However, the order also states, "in addition to the semiannual report, whenever a loss or theft occurs of consequence, that in the opinion of the [component's] Security Programs Manager can have serious ramifications, the Department Security Officer

³⁸ The initial reports (Forms FD-500) for all 212 losses were filed between October 1, 1999, and January 31, 2002. However, the actual dates when the losses occurred may have been before October 1, 1999. Appendix IV details the number of days between the loss of each weapon and the filing date of the Form FD-500.

³⁹ DOJ Order 2630.2A, *Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures*, dated October 4, 1977, paragraph 11.c.

shall be immediately notified telephonically, and followed up by a written report.”

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

| REPORTING PERIOD | DUE DATE | DATE SUBMITTED |
|-----------------------------|------------------|--------------------|
| June 1 to November 30, 1999 | January 31, 2000 | January 21, 2000 |
| December 1 to May 31, 2000 | July 31, 2000 | September 25, 2000 |
| June 1 to November 30, 2000 | January 31, 2001 | February 6, 2001 |
| December 1 to May 31, 2001 | July 31, 2001 | November 14, 2001 |
| June 1 to November 30, 2001 | January 31, 2002 | March 12, 2002 |

Source: Department Security Officer

Although the FBI submitted semiannual theft reports, we found that the reports 2000 and 2001 were submitted 56, 6, 106, and 40 days late, respectively.

More important, the FBI’s reports were substantially inaccurate. We reviewed the lost items identified in the semiannual reports for 1999, 2000, and 2001 and compared them to the FBI’s inventory records of lost and stolen weapons and laptop computers. According to the FBI’s inventory records, 359 weapons (232 functional and 127 “red handles”) were lost or stolen between June 1, 1999 and November 30, 2001; however, only 9 appeared on the semiannual reports. The FBI was unable to explain why the other 350 items were not listed on the semiannual reports.

According to the FBI’s inventory records, 152 laptop computers were lost or stolen between June 1, 1999 and November 30, 2001; however, only 26 appeared on the semiannual reports. Once again, the FBI was unable to explain why the other 126 items were not listed on the semiannual reports.

Indications of Public Harm

We conducted certain tests to determine if the FBI’s losses of weapons and laptop computers resulted in harm to the public through loss of classified or sensitive information or physical injury.

Weapons

We queried NCIC and the Bureau of Alcohol, Tobacco, and Firearms (ATF) National Tracing Center database regarding 276 lost or stolen FBI weapons.⁴⁰ Our purpose was to determine whether any law enforcement personnel recovered lost or stolen FBI weapons through investigation of subsequent illegal activity. When our queries identified weapons recovered by local police, we reviewed police department records to determine the circumstances of the recovery and the extent, if any, of harm to the public.⁴¹ Our query of the National Tracing Center database found that some lost FBI weapons were, in fact, used in the commission of crimes.

Two Weapons Stolen from a Special Agent's Residence

In September 1995, two firearms were stolen from the residence of a Special Agent in Baltimore, MD. One weapon had been left on the top shelf of a closet, partially covered by several sweaters, so that it would be accessible to the Special Agent in case of an emergency; the other was in a briefcase on the floor of the closet. (The briefcase also contained two extra fully loaded magazines, a loaded speed loader, and the cases for the magazines and speed loader.)

The theft occurred while the Special Agent was absent from the residence and his daughter was entertaining friends. When the daughter left the house briefly, her friends stole the weapons.

One weapon was recovered soon after the theft. In August 1996, Baltimore police retrieved the second firearm, a Smith and Wesson revolver, during the arrest of a felon in possession of a firearm. The subject had a long record of violent and criminal activity, including charges of murder, assault with intent to murder, handgun use in committing a felony, and possession and distribution of drugs.

An FBI report dated December 22, 1995, stated that the Special Agent "had taken reasonable care, in his absence, to secure these weapons in his home It is reasonable to conclude that . . . the weapons would not have been discovered in his home without an intrusive and extensive search

⁴⁰ See footnote 45.

⁴¹ The records in question identified additional weapons recovered by local police at crime scenes. After confirming that an FBI weapon was recovered, the FBI removed the weapon from the list of missing items. The weapons discussed in this section of the report had a "disposition date" after September 30, 1999.

by the subjects." As a result the Special Agent received counseling on the secure storage of weapons in his residence.

In our judgment, the FBI's response to the theft of these weapons was questionable. We do not agree that it was reasonable to store a weapon on a closet shelf with only a sweater to conceal it.

Stolen Revolver Recovered with 18 Bags of Marijuana

A Smith & Wesson revolver was lost or stolen under circumstances that are unclear. In March 1994, the New York field office reported the theft of the weapon in September 1993, shortly before the employee in question retired. Although we found indications that the weapon was stolen from an FBI vehicle, the FBI could not provide us with adequate details about the theft.

The FTU's index card for the weapon contained a notation dated January 27, 1994 stating the employee had retired and "did not return [the weapon] to Quantico. HQ notified." By itself, this notation could give the impression that the employee retained the weapon after retiring. However, as noted above, loss of this weapon occurred before the Special Agent's retirement.

The next notation on the FTU index card, dated August 3, 2000, stated "FD-500 submitted," indicating that a "Report of Lost or Stolen Property" was submitted more than six years after the theft occurred.

This was also six months after New York police recovered the weapon (in February 2000) from a defendant in a drug case. The defendant was charged with criminal possession of a weapon and unlawful possession of 18 bags of marijuana.

The FBI retrieved the weapon from the local police in February 2002.

Handgun Stolen from FBI Vehicle

This weapon was stolen from a Special Agent's assigned vehicle in December 1993. The Special Agent had left the weapon in the front locked console of the vehicle, which was parked in the driveway at the Special Agent's residence in Macon, GA. Someone broke the small window in the left side rear door of the vehicle, gained entry, and removed the weapon and three ammunition magazines. In September 1995, local police in Memphis, TN recovered the firearm when they arrested an individual for unlawful possession of a weapon.

In January 1994 the Special Agent received a Letter of Censure based on the loss of this firearm. The Letter stated in part, "Your failure to adequately safeguard this property is unacceptable. You should take precautions, to include properly safeguarding your property within your residence, to ensure there is no recurrence of loss by theft of government owned property."

The FBI's record relating to this firearm was inadequate. The index card maintained by the FTU contained a notation dated December 3, 1993, documenting issuance of the weapon to the Special Agent. The next entry was dated April 26, 2001, and read, "weapon reported stolen per FD-500 submitted from Atlanta dated 4/5/01." There was no explanation why a theft that occurred in December 1993 was not reported to the FTU by the field office until April 2001. We were also unable to determine why the FBI was unaware that local police recovered the weapon in September 1995. We learned of the recovery during our audit through a query of the FBI's own CJIS database.

FBI Weapon Found on Homicide Victim

A Glock handgun was stolen from the residence of a Special Agent in New Orleans, LA in September 2000. The available record shows that the burglar(s) gained entry to the residence by forcing open a side door that had been secured with a pad lock, a deadbolt lock, and a security chain. This suggests that the Special Agent had taken reasonable precautions to secure his residence; however, the record does not document how or where the weapon was stored within the residence. The FBI's Office of Professional Responsibility concluded that loss of the weapon did not result from negligence on the part of the Special Agent.

In September 2001, the weapon was recovered by New Orleans police officers from the pocket of a murder victim. We were unable to determine whether the victim or anyone else had ever used it to commit a crime.

Laptop Computers

The loss of classified or even sensitive information can result from the loss or theft of the FBI's laptop computers. To determine the risk of losing such information, it is necessary to consider the security environment within which the FBI's laptop computers operate. The MIOG outlines policy regarding laptop computers, including a provision that all FBI laptop computers are "authorized to process classified information up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET)."

In our judgment, the risk level in this environment is high because:

- every FBI laptop computer is authorized to process sensitive information and classified information up to the Secret level;
- every laptop computer is authorized to connect to FBINET;⁴²
- with written authorization, any laptop computer can be permitted to access Top Secret information; and
- laptop computers are portable.

After completing the final phase of its recent inventory on March 31, 2002, the FBI reported to us that 310 laptop computers were missing, of which 218 (70 percent) had an "unknown" security level and 92 (30 percent) were "unclassified." Since this information came to us after we completed our fieldwork, we did not test its validity. However, we are concerned by the FBI's determination that the security level of 70 percent of the missing laptop computers was unknown.

We cannot state with certainty whether sensitive or classified information was actually compromised by any of the thefts or losses of laptop computers, but we believe the potential certainly exists. There are no records documenting the data stored on those computers and, since they are missing, we have no way to determine what information they contained.

Although we cannot state with certainty that no Top Secret information was lost, we note that according to the FBI only five laptop computers were authorized in writing to process Top Secret information, and those computers were not among the ones lost or stolen.

⁴² FBINET is also authorized to process information up to the level of Secret.

Conclusions

During our audit review period of October 1, 1999 through January 31, 2002, the FBI reported the loss or theft of 212 functional weapons, 142 "red handle" training weapons, and 317 laptop computers. The circumstances surrounding these losses and thefts often included carelessness or failure to adhere to FBI policy, which indicates a need for the FBI to take forceful corrective action.

The FBI must improve its management of weapons and laptop computers. In particular, the FBI must foster an environment where the protection of sensitive assets, such as weapons and laptop computers, is given due emphasis by all employees.

In our judgment, the FBI must establish and adhere to firm deadlines for reporting of every lost weapon and laptop computer; investigation of these losses and thefts by OPR; and entry of required data into NCIC. The absence of such deadlines is a serious omission from FBI policy that undermines the requirement to report losses.

Recommendations

We recommend that the Director of the FBI:

1. Consider revising FBI policies to establish and enforce criteria by which employees will be disciplined when the employee's negligence results in the loss or theft of a weapon or laptop. This policy should also consider and set forth any circumstances under which employees will be held personally liable for the cost of the item.
2. Strengthen FBI policy regarding the proper storage of FBI property outside the office, in particular as it pertains to storing property at an employee's residence or in vehicles.
3. Establish and adhere to firm deadlines for: (a) employees to report the loss or theft of FBI property to their supervisors; (b) supervisors to report losses or thefts to Headquarters units, including the FTU, the OPR, and the Property Management Unit; (c) OPR to initiate and complete investigations; and d) designated employees to enter losses into NCIC (when appropriate).
4. Revise the Form FD-500 to include the date of loss/theft; the date the property was entered into NCIC and the resulting NCIC number; and the individual responsible for pooled property, such as unassigned weapons maintained in the armory.
5. Submit complete, accurate, and timely Department Semiannual Reports to the SEPS.

II. MANAGEMENT CONTROLS

The FBI failed to give sufficient priority to property management. The FBI did not complete a full physical inventory of accountable property between 1993 and 2001, despite its own policy requiring such inventories every two years. In our judgment, had the FBI completed the physical inventories initiated during the last ten years, the FBI could have identified problems earlier and initiated timely corrective action.

We also noted other weaknesses in the FBI's management controls. The FBI's financial system was not fully integrated with the PMA. A total of 105 weapons were lost or stolen from field office armories, but none were reported to OPR because OPR generally did not conduct an inquiry unless a specific individual could be named as the subject. In some instances, the FBI failed to recover issued weapons from separating employees. The documentation of the disposal of laptop computers failed to establish that all sensitive or classified information had been sanitized prior to disposal.

This section of the report examines the management controls employed by the FBI over weapons and laptop computers. We assessed the FBI's compliance with OMB Circular A-123⁴³ and Federal Property Management Regulations, as well as Department and FBI guidance. Our discussion addresses the following topics: Physical Inventories; Purchases; Receipt and Assignment; Pooled Property; Specialized Equipment and Rapid Mobilization Teams; Separated Employees; and Disposals.

Physical Inventories

Our most significant finding in the area of management controls involves physical inventories of accountable property. We found that the FBI

⁴³ OMB Circular A-123 defines management controls as "the organization, policies, and procedures used by agencies to reasonably assure that . . . programs and resources are protected from waste, fraud, and mismanagement A subset of management controls are the internal controls used to assure that there is prevention or timely detection of unauthorized acquisition, use, or disposition of the entity's assets." OMB Circular A-123, *Management Accountability and Control*, revised June 21, 1995, Attachment II, "Definition of Management Controls".

had not completed a full physical inventory of accountable property since sometime before 1993. According to information provided by the FBI:

- In 1991 and 1993 the FBI conducted manual physical inventories but there are no records available for them.
- In 1993, due to limited funding, the FBI purchased barcode equipment to begin physical inventories in the field divisions only.
- Due to technical problems with implementing the barcode technology, the 1993 physical inventories were delayed until 1994.
- The 1994 physical inventories continued to be hampered by technical problems, so in May 1995, the FBI acquired new barcode equipment that was distributed to the field divisions.
- The physical inventories were discontinued in August 1998 after the primary programmer was reassigned to another project. The inventories were 84 percent complete.⁴⁴
- On February 1, 1999, the FBI began a Bureau-wide physical inventory with an original deadline of June 1, 1999. Due to a delay in receiving additional barcode equipment, the deadline was extended to August 16, 1999.
- The 1999 physical inventory was discontinued on February 17, 2001; it was 99 percent complete for field divisions and 68 percent for Headquarters divisions.⁴⁵

The failure to complete these physical inventories was contrary to the FBI's own policy. The FBI's *Accountable Property Manual* states, "the FBI performs physical inventories of all property every two years."⁴⁶ The MAOP states more explicitly "each division must conduct a physical inventory of

⁴⁴ The percentage of completion is based on the number of items inventoried versus the total number of accountable property items on record. For example, when the 1993 inventory was discontinued (in 1998), 270,910 items from a universe of 321,580 had been inventoried (84 percent).

⁴⁵ The information provided to us by the FBI does not explain why the 1999 physical inventory was discontinued in February 2001; however, we note that according to the MAOP the next required biennial physical inventory was due to begin in that month.

⁴⁶ *Accountable Property Manual*, p. 48, Section 14-4.

issued personal property assigned to their employees during February of every odd-numbered year.⁴⁷

The 2001 biennial inventory began on June 27, 2001, with an initial deadline for completion of September 30, 2001. However, as a result of the terrorist attacks on September 11, 2001, that deadline was extended generally to November 15, 2001, and for some offices until December 17, 2001.⁴⁸ The final phase of the inventory, the inventory of issued personal property, was completed as of March 31, 2002. Since this was after the conclusion of our fieldwork, we were able to make only limited use of the results in our audit; we note, however, that the inventory disclosed that 423 functional weapons, 158 "red handles," and 310 laptop computers were lost or stolen (See Appendix VII for our summary of the results of this inventory).

The auditors who performed the FBI's annual financial statement audits have reported material weaknesses in procedures and management controls over property and equipment. For example, FBI procedures and controls do not provide adequate assurance that:

- Physical inventory results are properly recorded in the property management application and accounted for in the fixed asset control account in the general ledger (reconciliation).⁴⁹

In our judgment, the chronic failure to complete physical inventories of accountable property greatly undermined the FBI's ability to manage its assets. We recognize that the volume of accountable property in an organization the size of the FBI makes regular inventories difficult to accomplish, but it is precisely this volume that makes regular inventories essential for effective property management.

Items Tested

Our audit testing included an evaluation of the controls over property management activities specifically related to weapons and laptop computers

⁴⁷ MAOP, Section 6-10.2, paragraph (2) (a).

⁴⁸ The Boston, Newark, New York, and Washington field offices, as well as the Counterterrorism and Laboratory (Engineering Research Facility) Divisions received the longer extensions.

⁴⁹ OIG Audit Report 00-15, *Federal Bureau of Investigation Annual Financial Statement, Fiscal Year 1999*. This finding was repeated in the financial statement audit for the following year.

at FBI Headquarters and four field locations. In addition, we tested, on a sample basis, the accuracy and reliability of the FBI property records. The universe of weapons and laptop computers for the locations audited is displayed in Appendix VI, Table 1. In total, we reviewed 884 items, as summarized in the following table and detailed in Appendix VI, Table 2.

| TOTAL ITEMS REVIEWED | | | | | | |
|-----------------------------|--------------------------------|------------|--------------|-------------|------------|------------|
| | FBI Headquarters ⁵⁰ | Denver | Jacksonville | Los Angeles | New Haven | TOTALS |
| WEAPONS | 135 | 88 | 95 | 80 | 56 | 454 |
| LAPTOP COMPUTERS | 281 | 31 | 38 | 35 | 45 | 430 |
| TOTALS | 416 | 119 | 133 | 115 | 101 | 884 |

Purchases

Weapons

The purchase of all new weapons is controlled in the Firearms Training Unit (FTU) at the FBI Academy in Quantico, VA. The FTU requisitions new weapons, which are purchased by Procurement Officers in the Property Procurement and Management Section of the Finance Division. After receiving and verifying new weapons, the FTU sends the invoice package to the Commercial Payments Unit of the Finance Division for payment.

Upon delivery, the FTU receives the weapons, tests them, and enters them into the PMA, which is the official property management system for the FBI.⁵¹ The FTU also prepares an index card containing additional information beyond that in the PMA, such as the repair history of each weapon.

⁵⁰ Including Quantico, VA.

⁵¹ Our review of these activities found adequate segregation of duties among FTU staff members.

The FTU issues weapons to new Special Agents upon graduation from the Training Academy or transfers the weapons to the appropriate division or field office.

Our review of the FBI's purchasing of weapons did not disclose any deficiencies. We judgmentally selected 20 disbursements for the purchase of weapons since October 1, 1999, and we traced all the purchases to the accounting system. The disbursements related to the purchase of 5,023 weapons. For each disbursement reviewed, we selected up to five serial numbers of weapons and traced them to the PMA.⁵² We traced a total of 80 weapons and noted no discrepancies.

Laptop Computers

The purchase of laptop computers is decentralized. New laptop computers may be purchased through FBI Headquarters or locally by field offices. Field offices can generate their own purchase orders for laptop computers if the aggregate cost is \$10,000 or less; in some instances, field offices use a Government-issued credit card to purchase computers if the cost is \$2,500 or less.

Unlike weapons, which are all received initially at a central point, laptop computers may be shipped either to FBI Headquarters or to a field office. However, payment for the laptop computers is centralized in the Commercial Payments Unit of the Finance Division at FBI Headquarters.

The Supply Technician for the receiving office has the responsibility of ensuring that new laptop computers are entered into the PMA. According to FBI officials, the procedure for ensuring that all purchased property is entered into the PMA is entirely paper-driven. The Supply Technician generally relies on receipt of a copy of the receiving report and purchase documents. If the documents are misdirected, lost, or not submitted, the property might not be entered into the PMA. Further, property system data for non-capitalized accountable property is not manually reconciled with purchase data from the accounting systems.

Our review of the purchases of laptop computers identified one deficiency. From each of the 34 disbursements reviewed, we selected at least 5 serial numbers of laptop computers and attempted to trace them to the PMA. Of the resulting 225 items selected, the serial numbers for 11

⁵² We traced five weapons per disbursement unless fewer than five weapons were received, in which case we tested all weapons received.

(5 percent) were not found in the PMA.⁵³ In our judgment, the consequences of this omission are potentially serious because any accountable items not listed in the PMA could be lost or stolen and no inventory record would exist.

Reconciliation to Financial System

We determined that the FBI's financial system was not fully integrated with the PMA. As a result, the financial and property management systems did not automatically verify whether the number of items actually purchased agreed with the number of items placed into inventory. Because the reconciliation was not performed for non-capitalized property at the financial management level,⁵⁴ the property management system must rely on accounting information at the individual transaction level to ensure accuracy. At the time of our review, there was no requirement to ensure information was shared between the two systems.

The absence of this reconciliation control procedure decreases the level of reliability of the data in the property system, since the property system relies on non-accounting information and on the initiative of the property manager to determine what property was purchased. In our judgment, the reconciliation between the property and financial systems should be performed of weapons and laptop computers expensed in the financial system to ensure the accuracy of both systems. This reconciliation is consistent with the Joint Financial Management Improvement Program (JFMIP) Property Management Systems Requirements, which includes the property management system as part of an organization's overall financial management system. The JFMIP states that the goal of all system interfaces is to facilitate the reconciliation between property management and financial systems to ensure data accuracy.

⁵³ The 34 disbursements related to the purchase of 2,693 total laptop computers.

⁵⁴ For capitalized property, a reconciliation is performed between the financial system and the property system at the financial management level to determine the beginning and ending balances of ledger accounts, determine appropriate depreciation, and ensure the accuracy of the financial statements. A detailed reconciliation is not performed at this level for non-capitalized property because non-capitalized property is expensed during the course of the fiscal year and becomes indistinguishable, for financial reporting purposes, from other expenses.

Receipt and Assignment

Weapons

A document prepared by the FTU states that the FBI obtains firearms through: (1) direct purchase; (2) seizures and disposal actions by federal courts; (3) the Defense Re-utilization Management Office; (4) "riding" other federal agency contracts; (5) direct transfers from other federal agencies; and (6) other means authorized by the General Services Administration.

Newly ordered weapons are delivered to the FTU at the FBI Training Academy in Quantico, VA. At the FTU, the weapons are physically verified against the packing slip to assure that the serial numbers match. A Supply Technician then enters the weapons into inventory by: (1) preparing a 5 x 7 index card including the make, model, caliber, manufacturer, serial number, date of receipt, purchase order number, and price; (2) proofing the index card against the packing slip to assure that the index card was correctly prepared; (3) assigning FBI barcode numbers to each weapon and noting the barcode number on the index card; and (4) entering the weapons in the PMA.

Regarding the assignment of weapons to individual employees, FBI policy states, "All Bureau property such as credentials, badges, weapons, clothing, etc., issued and in the possession of an FBI employee must be maintained on the Bureau Personnel Management System, Issued Personal Property (IPP) System and Form FD-281, Receipt of Government Property, must be executed."⁵⁵ (See Appendix XIV.)

Our review of the receipt and assignment of weapons did not identify any significant deficiencies in this area.

Laptop Computers

Laptop computers are generally shipped directly from the vendor to the requesting office. The process for receiving new laptop computers includes matching the data on the packing slip to the purchase order and invoice. The end user and a supervisor sign the invoice to verify the number of laptop computers received. The signed invoice, packing slip, and receiving report are then sent to the Commercial Payments Unit at FBI Headquarters for payment. Supply Technicians at the appropriate Headquarters Division or Field Office enter new laptop computers in the PMA.

⁵⁵ MAOP, Part 2, Section 6-10.2.

Several provisions of the MIOG govern the assignment of laptop computers to employees:

- A Receipt for Government Property, Form FD-281, must be executed for laptop computers “issued to an individual for an extended period of time.”
- An FBI Property Pass, Form O-96 (see Appendix XVI), or a Charge-Out Record of Nonexpendable Property, Form FD-79 (see Appendix XVIII), may be used to account for laptop computers for shorter periods of time.
- “To the extent possible,” laptop computers “should be kept in the possession of the individual to whom they are issued or charged out.”⁵⁶

At the four field locations reviewed, the Supply Technicians or Principal Firearms Instructors used secondary systems to track items that were under their control on a day-to-day basis. The secondary systems included automated spreadsheets, database applications, and written lists. We were informed that these secondary systems were used to track individual assignments, make immediate changes to an item’s specific location, and enter additional information as needed to manage and track the property.

Accuracy of Property Records

To test the accuracy and completeness of the property records, we verified the existence of selected weapons and laptop computers appearing in the PMA. In addition, we selected a sample of weapons and laptop computers found at each location reviewed and traced them to the PMA. In total, we physically inspected 374 weapons and 205 laptop computers, as shown in the following table, and found no discrepancies. Further details of our sample, by property type, location, and type of test appear in Appendix VI, Tables 3 and 4.

⁵⁶ MIOG, Part 2, Section 35-9.4.6, paragraphs (2) and (3).

| ITEMS PHYSICALLY INSPECTED | | | | | | |
|-----------------------------------|------------------|------------|--------------|-------------|------------|------------|
| | FBI Headquarters | Denver | Jacksonville | Los Angeles | New Haven | TOTALS |
| WEAPONS | 55 | 88 | 95 | 80 | 56 | 374 |
| LAPTOP COMPUTERS | 56 | 31 | 38 | 35 | 45 | 205 |
| TOTALS | 111 | 119 | 133 | 115 | 101 | 579 |

Armory Weapons

At each of the sites audited, the Principal Firearms Instructor was responsible for unassigned weapons that were available for special assignment or issuance as needed. These weapons were physically secured either in a vault, in a cage within a vault, or in a separate armory building. Physical safeguards such as alarms, numeric keypads, and combination locks were used to limit access to the physical area and to secure the weapons. According to FBI policy, pooled weapons are temporarily assigned to individuals using the hand receipt system.

However, our work at Los Angeles disclosed that until late in 1998 the Field Office had relied on an "honor" system for charging weapons out from the armory. Although Special Agents must now sign for such weapons, we believe that the prior reliance on the "honor" system contributed to the FBI's inability to locate weapons.⁵⁷

Complicating the situation in Los Angeles, a Principal Firearms Instructor (PFI) who retired in 1997 kept records using an informal system that relied on loose scraps of paper. Consequently, his successors had considerable difficulty in determining the whereabouts of field office weapons. As of March 1998, the successor PFI could not account for 150 weapons. After a thorough inventory, the number of missing weapons was reduced from 150 to 16, 2 of which were referred to OPR to determine whether an OPR investigation should be initiated. According to the Los Angeles Field Office, the loss of the remaining 14 weapons was "entirely

⁵⁷ A memorandum dated August 24, 2001, from the FTU indicated that other offices also relied on the "honor system"; however, the memorandum did not identify which offices.

attributable to the negligence of former PFI [name] and his superiors, all of whom are now retired.”

During the period from October 1, 1999 through January 31, 2002, a total of 105 of the 212 missing weapons were either lost or stolen from field office armories nationwide. We determined that none of those losses were reported to the OPR because OPR generally does not conduct an inquiry if there is no realistic likelihood of identifying a current employee as the subject.

Pooled Laptop Computers

Each of the offices we audited had pooled laptop computers. According to the Supply Technicians, the process for temporarily issuing the laptop computers using hand receipts was the same as for the pooled weapons. Like weapons, the laptop computers were stored in controlled space. Our review did not disclose any significant problems with pooled laptop computers at the offices we audited.

Specialized Equipment and Rapid Mobilization Teams

The FBI has a Critical Incident Response Group (CIRG), which is a tactical unit housed near the Training Academy in Virginia. The FBI also has a Hostage Rescue Team (HRT), based in Quantico, VA, and SWAT teams assigned to each field office. Special weapons, such as MP-5 submachine guns and .45 caliber pistols, are assigned to the various offices, which issue them to individual team members by means of a hand receipt. The local Principal Firearms Instructor (PFI) controls weapons maintained in the armory, while the individual Special Agents are responsible for the custody and storage of issued weapons in their possession.

At the FBI Academy in Quantico, VA, we tested controls over weapons assigned to the HRT and found no discrepancies.

Separated Employees

The process for separating employees from the FBI includes an exit interview with the employee’s supervisor and completion of certain forms. FBI procedures call for the supervisor to review the PMA printout for the employee and recover all issued property listed on that document.

In addition, the supervisor is supposed to complete a Report of Exit and Separation (Form FD-193) and a Receipt for Government Property (Form FD-281). The Form FD-193 documents a variety of actions that must

be completed upon separation of an employee, including the following (See Appendix XIII).

- The person conducting the exit interview must check “yes” or “no” next to the statement, “employee has been afforded a debriefing by his/her respective Security Officer.” If the answer is “no,” an explanation must be provided.
- The person conducting the exit interview must also check “yes” or “no” next to the statement, “all Government property, documents made or received while in the FBI’s service . . . will be collected on date employee ceases active duty”
- Departing employees must separately sign four statements, one of which reads “I understand that Federal Law prohibits former Government employees from retaining Government property, including classified and/or sensitive information. I understand that I may be prosecuted for possession of classified (as defined in MIOG, Part II, Section 26) or sensitive (as defined in MIOG, Part II, Section 16-18.8.1(1)) information. I affirm that I have returned all classified and/or sensitive information in my custody.”

The Form FD-281 is used for both receiving and returning government property. The portion of the form used for documenting the return of property has lines enumerating several items, including “Laptop Computer [Number].” However, we noted that the FD-281 does not have a space for documenting the return of weapons.

We judgmentally selected for review the files of 98 separated employees to determine whether all their assigned weapons and laptop computers were returned.⁵⁸ We found one discrepancy.

- During our testing at the New Haven field office, we determined that the whereabouts of one firearm issued to a former Special Agent were unknown. The Special Agent was assigned to the New Haven field office in December 1998, received a temporary transfer to San Antonio, TX, early in 1999 because of family hardship, and resigned in November 1999. The Special Agent apparently did not turn in the firearm and, as of January 2002, the FBI had not located it.

⁵⁸ The FBI’s property assignment records showed that these 98 former employees had been issued a total of 164 weapons and 31 laptop computers.

We also found other indications that the FBI might not be recovering all issued weapons from employees before separation.

- On August 10, 2001, the FBI sent a letter to former Special Agents “who had Bureau-issued firearms stolen or misplaced prior to their separation” from the FBI. The letter stated, “While the FBI knows that former Agents have made good faith efforts to locate these missing weapons, we must all acknowledge the possibility that some weapons may have been inadvertently taken home, placed in storage while personal belongings were being moved, and simply forgotten.” The letter then requested that the Special Agents in question “conduct another thorough search of their homes, vehicles, and all other areas where personal belongings are stored. Weapons that are located can be turned in to any local FBI office without further inquiry.” As a result of this effort at least one former Special Agent located a missing firearm and turned it in.
- In June 2001, the FTU determined that 31 firearms assigned to separated Special Agents were not accounted for, and not reported in the PMA as lost or stolen. Upon completion of the inventory of issued personal property (March 31, 2002), the FTU reported that 13 of those 31 firearms had been located, 16 were lost, and 2 were stolen.

An incident that happened in July 2001 resulted in adverse publicity for the FBI. The FBI could have averted this adverse publicity if it had exercised greater care in the recovery of issued weapons from the family of a deceased Special Agent.

Two FBI Weapons Recovered from Scene of an Accidental Shooting

Two FBI-issued handguns were recovered, together with a personally owned handgun, from the scene of an accidental shooting in Prince William County, Virginia, in July 2001. All three firearms were formerly assigned to a deceased Special Agent. The personally owned weapon had been used in the shooting and all three weapons had been stolen from the residence of the deceased Special Agent. The following chronology is based on information in FBI records and the local police report.

- The Special Agent died on April 27, 2001.
- On May 11, 2001, another Special Agent went to his residence to retrieve his Government-issued property. However, this Special Agent took with him a property list that did not include the

deceased Special Agent's two FBI-issued firearms. The deceased Special Agent's widow turned over various items, including a Glock 27 pistol, which she incorrectly believed was the one her late husband routinely carried. She believed it was the firearm issued to him by the FBI. However, that Glock was actually a personally owned weapon. The deceased Special Agent's two FBI weapons remained in the house.

- On June 27, 2001, the widow moved from Woodbridge, Virginia, to Richmond, Virginia. At an unknown time prior to that date, some teenagers, who were acquaintances of the deceased Special Agent's daughter, stole weapons from her house, including the FBI-issued weapons. They had located the key to the Special Agent's gun safe, opened it, and removed the weapons.
- On July 9, 2001, the FBI was informed that the two FBI weapons assigned to the deceased Special Agent had been recovered by local police at the scene of an accidental shooting in Prince William County, Virginia.

The loss of the two FBI weapons could have been prevented if the Special Agent who went to the residence of the decedent had with him a complete and current list of the late Special Agent's issued property.

Disposals

Weapons

Excess firearms, which are generally obsolete, are destroyed. The division or field office possessing an excess weapon initiates a "Declaration of Excess" form and an "Excess Property Detail Report," both of which are PMA transactions, plus a "Transfer Order – Excess Personal Property" (Standard Form 122) to transfer the weapon to the FTU (see Appendix XVII). The FTU notifies the Property Management Unit (PMU), which can authorize the FTU to proceed with the destruction. Groups of approximately 500 excess weapons are transported from the FTU's location in Quantico, VA, to a foundry where they are melted down in a process witnessed by FBI agents. The FTU then submits a "Requirements And Certification For Cannibalization And Destruction Of Equipment" (Form FD-519) to the PMU, which updates the PMA to reflect the destruction. (See Appendix XV.)

Our audit determined that the existing management controls over the destruction of weapons were well defined and carefully followed. Therefore, we limited our testing to 10 weapons from 547 listed on a Form FD-519

dated May 31, 2001, and we confirmed that the PMA accurately reflected their status as destroyed.

Laptop Computers

Field offices initiate the disposal of excess laptop computers by entering a "Declaration of Excess" and an "Excess Property Detail Report" into the PMA and by submitting a Form FD-519 to the Property Management Unit (PMU) at FBI Headquarters. The PMU authorizes donation or destruction of the laptop computers, as appropriate.

The destruction of defective or obsolete laptop computers involves taking certain measures to prevent the loss of sensitive information. The MIOG states,

Microcomputer equipment which has processed sensitive or classified information may not be released from FBI control until the equipment is sanitized and declassified. When inoperable, diskettes, tape cartridges, printouts, ribbons, and similar items used to process sensitive or classified information must be destroyed as classified trash. When inoperable, hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal.⁵⁹

A policy statement issued August 8, 1997, further states, "Before any hard drive can be released from FBI controlled space, it must be sent to FBIHQ to be degaussed."

At FBI Headquarters, we obtained a list of laptop computers excessed since October 1, 1999 and we tested a judgmental sample of ten. We traced them to the PMA and/or the Forms FD-519, and confirmed they had been excessed. However, the documentation provided to us did not address the subject of classified information and, consequently, did not establish that the computers in question were free of classified information. For all sites where we audited, both at FBI Headquarters and in the field, the available documentation did not establish that the hard drives had been properly destroyed. Responsible officials at each of those locations told us they believed that excess laptop computers and hard drives had been properly disposed of. However, the available records did not document their disposal and/or destruction.

⁵⁹ MIOG, Part II, Section 35-13.

For example, at the New Haven field office, we could not determine if all hard drives had been removed from obsolete or excess laptop computers. We found evidence that some laptop computers had been destroyed, but there was no documentation to show that the hard drives were removed and forwarded to FBI Headquarters. We did observe a number of hard drives in boxes kept in a secured area, but no record existed to trace those hard drives to any particular laptop computer. Consequently, we cannot be certain that proper procedures were followed in the disposal of laptop computers and hard drives.

Conclusions

The FBI must strengthen the management controls over weapons and laptop computers. A critical first step in that direction would be to adhere to the requirement to inventory accountable property every two years. To strengthen the controls further, we believe that the FBI should inventory sensitive items, including weapons and laptop computers, annually.

The FBI must also improve the process of recovering property from employees before they leave government service. Employees who cannot account for issued property when they leave the FBI should be subject to pecuniary liability for the missing item(s).

In the absence of sufficient documentation, we cannot determine whether excess laptop computers and components such as hard drives were destroyed according to FBI policy. As a result, we cannot be sure that sensitive information was not compromised. For this reason, the FBI must improve its documentation of the disposal of excess laptop computers and hard drives.

Recommendations

We recommend that the Director of the FBI:

6. Ensure completion of future inventories of accountable property every two years.
7. Annually inventory sensitive items, including weapons and laptop computers.
8. Implement a policy to reconcile non-capitalized property between the financial and property systems to ensure that the number of items acquired agrees with the number of items placed into inventory.
9. Strengthen the exit processing for separating employees to ensure that they turn in all issued property or reimburse the Government for any missing issued property.
10. Improve the documentation of the destruction of excess laptop computers and hard drives.