THE FEDERAL BUREAU OF INVESTIGATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS FOLLOW-UP AUDIT

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 07-18

February 2007

THE FEDERAL BUREAU OF INVESTIGATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS FOLLOW-UP AUDIT

EXECUTIVE SUMMARY

In 2001, the Attorney General requested that the Office of the Inspector General (OIG) conduct audits of the controls over weapons and laptop computers throughout the Department of Justice (DOJ) to address concerns about the DOJ's accountability for such property. In response, the OIG conducted separate audits of the controls over weapons and laptop computers at the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Federal Bureau of Prisons (BOP), and the United States Marshals Service (USMS). Audit reports on each component, including the FBI, were issued, as well as an overall report summarizing the results from each audit.[1]

The OIG's 2002 report on the FBI disclosed significant losses of weapons and laptop computers and examined the adequacy of the FBI's response to these losses. The report concluded that the FBI's procedures to prevent the loss of such equipment were not adequate. Specifically, we found that the FBI:

- identified 212 functional weapons, 142 inoperable training weapons, and 317 laptop computers as lost, missing, or stolen for our 28-month review period.

- did not always report the missing items to the DOJ or enter lost and stolen weapons and laptop computers into the National Crime Information Center (NCIC) database.[2]

- did not have policies in place that required reporting lost or stolen laptop computers to its Office of Professional Responsibility (OPR), nor was the FBI investigating the loss of this equipment in a timely manner.

- had not established deadlines for reporting losses, was not conducting physical inventories as required, and was not reconciling its property records to its financial records.

---

[1] Department of Justice, Office of the Inspector General. Audit Report 02-27, *The Federal Bureau of Investigation's Control over Weapons and Laptop Computers*, August 2002.

[2] NCIC is a computerized index of criminal justice information, including criminal history information, fugitives, stolen property, and missing persons, that is available to federal, state, and local law enforcement and other criminal justice agencies.

- did not ensure that exit procedures were regularly followed for separating employees to ensure that they returned all issued property, including FBI-issued weapons.

- could not provide documentation to establish whether excessed laptop computers were properly disposed of as required.

To help address these deficiencies, we made 10 recommendations, including that the FBI establish firm deadlines for reporting lost or stolen weapons and laptop computers. The FBI agreed with each of our recommendations and outlined a plan for taking corrective action.

Follow-up Audit

We conducted this follow-up audit to assess the progress of the FBI in addressing the deficiencies regarding control over weapons and laptops. The FBI had the greatest number of losses, as well as the most significant deficiencies in controls, of all the DOJ components we reviewed in our 2002 audits.[3]

The objective of this follow-up audit was to determine whether the FBI has implemented adequate corrective action to the findings in the original audit report.[4] To conduct this follow-up audit, we interviewed FBI officials, reviewed documents, and tested controls at FBI Headquarters in Washington, D.C., the FBI Training Academy at Quantico, Virginia, and FBI field offices in Chicago, Illinois; Los Angeles, California; Miami, Florida; New York, New York; and Washington, D.C. Fifty-two percent of the FBI's 52,263 weapons and 54 percent of its 26,166 laptop computers were assigned to these offices.[5]

To determine whether the FBI has made progress in reducing its number of lost and stolen weapons and laptop computers, we compared the

[3] The problems in the Immigration and Naturalization Service (INS) were comparable, but INS functions were transferred to the Department of Homeland Security in 2003.

[4] Appendix I contains more information on the current audit's objectives, scope, and methodology.

[5] Appendix II contains more information on the current audit's sampling design.

rate of loss identified in our 2002 audit to the rate found in this follow-up audit. Our prior audit found that over a 28-month period the FBI reported 354 weapons and 317 laptop computers as lost or stolen. Our follow-up audit found that over a 44-month period the FBI reported 160 weapons and 160 laptop computers as lost or stolen. We determined that, except for stolen laptop computers, the rate of loss for each property category decreased, as detailed below.[6]

[6] Because the audit periods were different lengths, we analyzed the rate of loss on a monthly basis.

MISSING WEAPONS AND LAPTOP COMPUTERS
2002 AUDIT VS. FOLLOW-UP AUDIT[7]

Category	Number of Lost or Stolen Items Reported		Losses Reported Per Month	
	2002 Audit (28 Month Period)	Follow-up Audit (44 Month Period)	2002 Audit	Follow-up Audit
Lost Functional Weapons	107	48	3.82	1.09
Stolen Functional Weapons	105	94	3.75	2.14
Lost Training Weapons	142	18	5.07	0.41
Stolen Training Weapons	0	0	0	0
Total Lost or Stolen Weapons	***354***	***160***[8]		
Lost Laptop Computers	300	116	10.71	2.64
Stolen Laptop Computers	17	44	0.61	1.00
Total Lost or Stolen Laptops	***317***	***160***		

Source: OIG analysis of FBI data

Yet, despite the FBI's progress in decreasing the rate of loss for weapons and laptops, the FBI still reported 160 weapons and laptops that were lost or stolen. We recognize that in an organization the size of the FBI, some weapons and laptops will inevitably be stolen or go missing. However, it is important that the FBI take appropriate steps to minimize these losses. When losses occur, the FBI must timely report the loss, be able to identify the contents of lost laptops, and determine whether the laptop is encrypted. In addition, the FBI must investigate these losses and thefts, enter required

[7] Our review period for the 2002 audit covered 28 months, from October 1, 1999, to January 31, 2002. Our review period for our follow-up audit covered 44 months, from February 1, 2002, to September 30, 2005.

[8] The FBI objected to the inclusion of 43 of these 160 weapons because while they were reported as lost or stolen during our 44 month follow-up period, the loss actually occurred before our follow-up period. We did not delete these weapons from the table because: (1) the losses were not categorized as such in the FBI's official property management system until after the beginning of our follow-up period, (2) our approach in the follow-up audit was consistent with our approach in the 2002 audit, which also included weapons that were reported as lost or stolen during our review period, (3) none of these 43 weapons were included in the 354 lost or stolen weapons reported in the 2002 audit, (4) to delete them would give the appearance that the FBI had 43 fewer lost or stolen weapons than was actually the case.

data into the National Crime Information Center (NCIC), and report the losses to DOJ as required.

Our audit found that the FBI has not taken sufficient corrective action on several recommendations outlined in our 2002 audit report to address the issue of missing and stolen equipment. Perhaps most troubling, the FBI could not determine in many cases whether the lost or stolen laptop computers contained sensitive or classified information. Such information may include case information, personal identifying information, or classified information on FBI operations.

Prior to our follow-up audit the FBI did not maintain records indicating which of its laptop computers actually contained sensitive or classified information. Moreover, during this follow-up review, the FBI could not identify for us the contents of many of the lost and stolen laptops, including whether they contained sensitive or classified information.

The following sections of this Executive Summary summarize the main findings of this follow-up audit.

Reporting Weapons and Laptop Losses

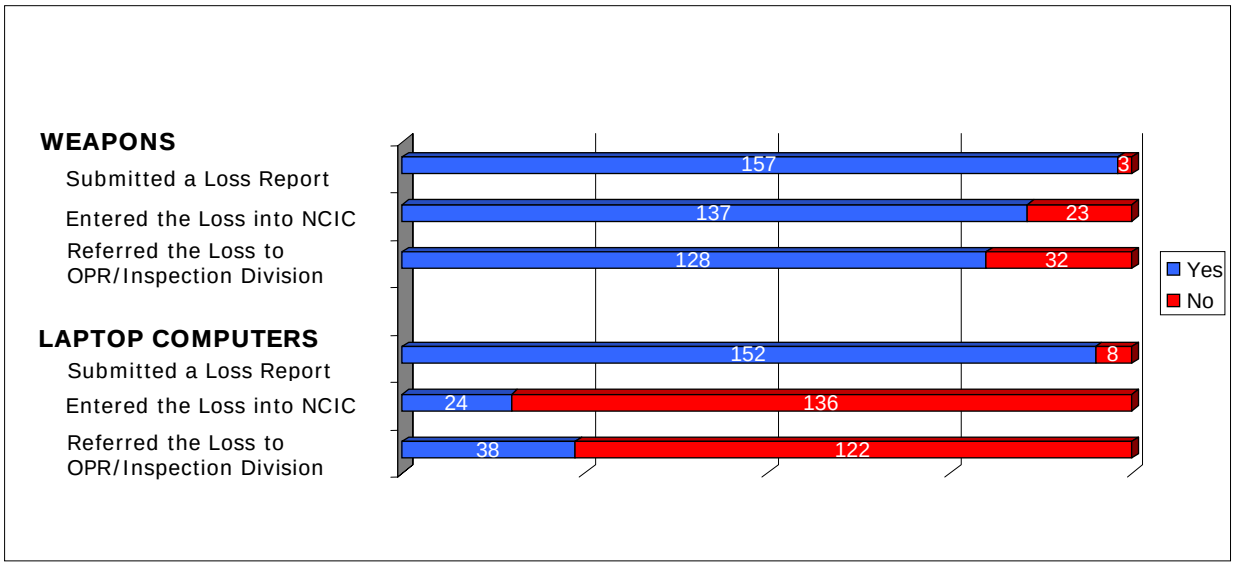
During our initial review in 2002, we found that the FBI did not specify deadlines for submitting the Report of Lost or Stolen Property form (Form FD-500) to report the loss of FBI property. As a result, we recommended that the FBI establish and adhere to firm deadlines to ensure that: (1) employees promptly report the loss or theft of FBI property to their supervisors; (2) supervisors report losses or thefts to headquarters units, including the Firearm Training Unit (FTU), OPR, the Asset Management Unit, and the Security Division; (3) OPR initiates and completes an investigation into the loss; and (4) information from the Form FD-500 is entered into NCIC (when appropriate).

In response, the FBI revised its policy to require that employees report lost or stolen weapons and laptop computers to their division office within 5 days after discovery of the loss. Division offices, in turn, are required to submit a Form FD-500 to the FBI's Finance Division and the Asset Management Unit within 10 days of the loss. All losses of weapons and

laptop computers are required to be entered into the NCIC database and forwarded to the FBI Inspection Division for investigation.[9]

We reviewed the reporting actions taken by the FBI in response to lost or stolen weapons and laptop computers by examining the Forms FD-500 during our 44-month review period. We assessed whether the loss was reported to the Asset Management Unit, entered into NCIC, and referred to the Inspection Division for investigation and OPR for adjudication. The table below categorizes our findings.

FBI REPORTS OF THE LOSS OR THEFT OF WEAPONS AND LAPTOP COMPUTERS FEBRUARY 1, 2002, THROUGH SEPTEMBER 30, 2005



Source: OIG analysis of FBI data

Of the 160 missing weapons, the FBI was able to provide Forms FD-500 for 157 weapons. The remaining three weapons were missing the required form. Of the 157 lost or stolen weapons that were reported using a Form FD-500, we found:

- 18 weapon losses were reported using an outdated Form FD-500. The old form did not capture critical information such as the date of loss, NCIC entry, and whether OPR was notified.[10]

[9] Since the issuance of our initial audit report in 2002, the FBI reorganized OPR and the Inspection Division. In February 2004, the FBI transferred the responsibility for investigations of alleged employee misconduct from OPR to the Inspection Division. The OPR continues to be responsible for adjudicating disciplinary matters.

[10] The Form FD-500 was updated on July 24, 2002, to include new fields. An additional 47 FD-500's submitted prior to July 24, 2002 did not contain critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 92 weapon losses were reported on the new Form FD-500. However, 51 of the 92 new Forms FD-500 were incomplete because the individual preparing the form did not enter critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 54 weapon losses were reported late—more than the required 10 days—thus possibly delaying timely investigation into the circumstances of the loss.

Of the 160 missing laptop computers, the FBI was able to provide Forms FD-500 for 152 laptops. Eight laptops were missing the required form. Of the 152 that were reported using a Form FD-500, we found:

- 24 laptop losses were reported using an outdated Form FD-500.[11] The old form did not capture critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 107 laptop losses were reported on the new Form FD-500. However, 82 of the 107 new Forms FD-500 were incomplete because the individual preparing the form did not enter critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 38 laptop losses were reported late—more than the required 10 days—thus possibly delaying timely investigation into the circumstances of the loss.[12]

Thus, although the FBI has strengthened its policy for reporting lost or stolen weapons and laptop computers by revising the Form FD-500 and establishing a new 10-day deadline for reporting losses, the FBI did not ensure that its staff always used the revised form or reported the loss within 10 days, as required. We recommend that the FBI ensure that its staff prepare complete and accurate loss reports using the latest version of the Form FD-500 and submit those reports to the appropriate offices in a timely manner.

Contents of Lost or Stolen Laptop Computers

Our review of the 152 Forms FD-500 for lost and stolen laptops revealed that 101 were identified as not containing sensitive or classified information, 43 were not marked as either containing or not containing

[11] An additional 21 Forms FD-500 submitted prior to July 24, 2002 did not contain critical information such as the date of loss, NCIC entry, and whether OPR was notified.

[12] For more detail on the lost and stolen weapons and laptops, see Appendices III through VI.

sensitive or classified information, and 8 were marked as containing sensitive or classified information.[13]

We asked the FBI's Security Division for any additional information that it had on the 160 laptop losses. We were provided limited information on only 12 laptop losses that the Security Division had reviewed. Two of the 12 laptop losses that the Security Division reviewed were initially part of the 101 that were identified on the Forms FD-500 as not containing sensitive or classified information. The Security Division determined that these two laptop computers contained sensitive but unclassified information. Therefore, we added these two laptop losses to the eight that were identified on the Forms FD-500 as containing sensitive or classified information. Details related to the 10 laptops are provided in the table below.

[13] In addition to the 43 laptop losses for which the Forms FD-500 were not marked to indicate whether the laptops contained or did not contain sensitive or classified information, there were 8 laptop losses for which the Property Management Unit did not retain the Forms FD-500 and had no information on whether these laptops contained or did not contain sensitive or classified information. Therefore, we combined these 8 laptop losses to the 43 and discuss the FBI's response to these losses in more detail later in our report in the 51 Laptop Losses section.

DETAIL ON LAPTOP LOSSES
CONTAINING SENSITIVE OR CLASSIFIED INFORMATION

No.	Date of Loss	Office Reporting Loss	Type of Loss	Encrypted?	Nature of Contents
1	07/12/02	Boston Field Office	Stolen	Yes	Software for creating identification badges.
2	09/02/02	Indianapolis Field Office	Lost	Unknown	Unknown
3	09/24/02	New Orleans Field Office	Stolen	Unknown	Used to process surveillance-related electronic digital imaging.
4	07/15/03	Phoenix Field Office	Lost	Unknown	Unknown
5	03/11/04	Security Division	Stolen	Yes	System security plan for an electronic access control system.
6	05/19/04	Washington Field Office	Lost	Unknown	Unknown
7	05/06/05	Security Division	Lost	Unknown	Unknown - SCU determined contents to be sensitive, but unclassified.
8	06/24/05	CJIS Division	Stolen	Yes	Unknown - SCU determined contents to be sensitive, but unclassified.
9	08/21/05	San Diego Field Office	Stolen	Unknown	Unknown - SCU determined contents to be sensitive, but unclassified.
10	Unknown (approx. 07/02)	Quantico Laboratory Division	Stolen	Unknown	Names, addresses, and telephone numbers of FBI personnel.

Source: FBI Forms FD-500

Although 8 of the 10 laptop losses were identified on the Forms FD-500 as containing sensitive or classified information, the Forms FD-500 for these eight laptop losses did not specifically make a distinction as to whether the information was sensitive or classified National Security Information (NSI).[14] We asked FBI Asset Management Unit and Security Division officials whether they could identify if any of the eight laptops did in fact contain National Security Information. The Security Division provided us information to indicate that the laptop loss reported by the CJIS Division on June 24, 2005, contained sensitive but unclassified information.

[14] According to the FBI Security Handbook, 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. Classified information (National Security Information) 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. For further details on the classification levels of Classified National Security Information see Appendix XVII.

However, FBI officials informed us that they did not know whether the remaining seven laptops that were identified as containing sensitive information actually contained classified information.

According to the OPR and Inspection Division records, the FBI investigated 6 of the 10 laptop losses that were known to contain sensitive or classified information. Of the six laptop losses that were investigated, one resulted in a 3-day suspension, two investigations were pending as of February 2006, and three resulted in no action taken against the employee. The FBI did not investigate the remaining four losses, including the loss of laptop computers that contained personal identifying information of FBI personnel and software for creating identification badges.[15]

Similarly, we asked FBI Security Division officials if they conducted any type of review to determine the contents of the remaining seven laptop losses or to assess the potential damage to national security and the FBI's operations. Security Division officials stated that they are reviewing the Forms FD-500 and contacting the appropriate field offices to determine what kind of information was on the laptops. However, the Security Division officials informed us that because these losses occurred some time ago it is doubtful that the FBI would still have information about the content of the laptops.

51 Laptop Losses

As noted above, the Forms FD-500 for 43 of the 51 laptop computers did not indicate, as required, whether the laptops contained sensitive or classified information. The employees who completed the forms did not check the box to indicate whether sensitive or classified information was on the laptop, nor did the Accountable Property Officer or the Asset Management Unit complete that section of the form when it was submitted. Moreover, the forms that were completed did not contain an adequate description of the information contained on the laptops. See Appendix IV. An analysis of the 51 laptop computers is provided in the table below.[16]

[15] See Appendix IV for a detailed description of the disciplinary action taken relating to the 160 FBI laptops that we identified in our follow-up audit as being lost or stolen.

[16] A more detailed analysis can be found in Appendix VII.

ANALYSIS OF THE 51 LAPTOP COMPUTERS UNKNOWN TO HAVE SENSITIVE OR CLASSIFIED INFORMATION

Category	*Assigned To Employee*	*Unassigned*	*Total*
Unexplained Losses[17]	3	22	**25**
Loss Identified During FBI Physical Inventories	5	16	**21**
Stolen from Vehicle	1	1	**2**
Stolen from FBI Office	0	1	**1**
Other	2	0	**2**
TOTAL	**11**	**40**	**51**

Source: FBI Forms FD-500

Seven of these 51 laptop computers were assigned to divisions within the FBI that handle some of the most sensitive information related to national security. Six were assigned to the Counterintelligence Division and 1 was assigned to the Counterterrorism Division. Yet, the FBI did not know the contents of these computers or whether they contained sensitive or classified information.

Of these 51 laptops, 11 were referred to FBI's OPR/Inspection Division. Two resulted in disciplinary action of the employee -- one letter of censure and one 3-day suspension. The documentation maintained at OPR/Inspection Division did not indicate the contents of these laptop computers.

This is a significant deficiency. Some of these laptops may have contained classified or sensitive information, such as personally identifiable information or investigative case files.[18] Without knowing the contents of these lost and stolen laptop computers, it is impossible for the FBI to know the extent of the damage these losses might have had on its operations or on national security.

FBI officials acknowledged to the OIG that there was a breakdown in obtaining the necessary information on the contents of the laptops that were lost or stolen. They suggested that part of the cause may be attributed to

[17] Eight of these 22 laptops were not assigned to an employee.

[18] Personally Identifiable Information is information about an individual maintained by an agency, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history, as well as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, or other personal information which is linked or linkable to an individual.

the lack of a centralized office in the FBI that could ensure that Forms FD-500 are complete and accurate.

Entering Losses of Weapons into NCIC

FBI policy states that lost and stolen weapons and laptops are required to be entered into NCIC. Our 2002 audit found that 14 of the 276 (5 percent) lost or stolen FBI weapons had not been entered into NCIC. Entering these items into NCIC could increase the chance of recovering the weapon or identifying the weapon if it is used in the commission of a crime.

In our follow-up audit, we found no NCIC records for 23 of the 160 (14 percent) lost or stolen weapons and no NCIC record for 136 of the 160 (85 percent) lost or stolen laptops.[19] At our exit conference, FBI officials stated that 10 of the 23 weapons currently do not have a record in NCIC. The remaining 13 included 6 weapons that had active records and 7 weapons that have been recovered.

We also queried NCIC to determine whether the lost and stolen weapons and laptop computers were recovered and, for the weapons, whether they were used in the commission of a crime. We identified no instances where law enforcement recovered any of the 160 lost or stolen weapons the 160 lost or stolen laptop computers. However, after completion of our fieldwork, the FBI reported to us that seven weapons had been recovered. Details of those weapons are listed in Appendix III.

Referring and Investigating Losses

Our 2002 audit found that losses of weapons and laptops were not regularly referred to OPR for investigation and that disciplinary action was generally not taken when individuals deviated from FBI policies concerning the handling of weapons and laptops. As a result, we recommended the FBI revise its policy and establish criteria for disciplining employees whose negligence resulted in the loss or theft of a weapon or laptop.

In response to our recommendation, the FBI stated that all weapon and laptop losses are required to be referred to OPR/Inspection Division. In our follow-up audit, we reviewed documentation related to OPR's and the Inspection Division's investigations. The results follow.

[19] In our prior audit, we did not determine whether lost or stolen laptop computers were entered into NCIC because at the time the FBI had no requirement to enter this information into NCIC.

Weapons Loss

The MAOP requires that each weapon loss must be referred to OPR. However we found that 32 weapons (20 percent) were not referred. Further, of the total 160 lost or stolen weapons OPR/Inspection Division opened an internal investigation into 70 (43 percent) of those losses. OPR/Inspection Division explained that it did not open an internal investigation for the remaining 90 losses for the following reasons:

- 22 losses did not receive requisite notification from field offices
- 58 had no evidence of employee misconduct that would warrant an internal investigation
- 10 were training weapons

We found it troubling that many of the weapon losses were not referred to OPR/Inspection Division for investigation even though the requirement in the MAOP clearly states that each weapon loss must be referred to OPR. As we previously mentioned, FBI officials told us that they do not investigate these losses because of insufficient information to indicate possible misconduct or negligence by an employee or the fact that the weapon was not specifically assigned to an employee.

Laptops Loss

The MAOP requires that each laptop loss must be referred to OPR. We found that 122 laptops (76 percent) were not referred. Further, of the total 160 lost or stolen laptops OPR/Inspection Division initiated an internal investigation into 21 (13 percent) of the losses. OPR/Inspection Division explained that it did not initiate an internal investigation for 139 losses because of the following reasons:

- 122 losses did not receive requisite notification from field offices
- 17 had no evidence of employee misconduct that would warrant an internal investigation

Similar to lost or stolen weapons, OPR/Inspection Division explained that cases are opened when there is sufficient evidence of an employee's

misconduct, and that cases were not opened if the lost or stolen laptop was not assigned to specific FBI personnel.[20]

Lack of Centralized Oversight and Monitoring

In our analysis of the FBI's response to lost and stolen weapons and laptop computers, we identified several weaknesses that resulted in inadequate reporting of weapon and laptop losses within the FBI. When reports were submitted, there did not appear to be any type of review at the FBI's Asset Management Unit to ensure that all necessary information and documentation was received. Also, there did not appear to be consistent notification to the proper headquarters units, such as the Security Division or the OPR/Inspection Division.

INTERNAL CONTROLS

In our 2002 audit, we reported that the FBI failed to give sufficient attention to property management. Periodic inventories of accountable property were not conducted, departing employees did not always return all property that had been issued to them, and the destruction of outdated, damaged, or excessed laptop computers was not adequately documented. Additionally, while the FBI documented the disposal of laptop computers, it did not adequately document that all sensitive or classified information had been sanitized prior to their disposal.

In our follow-up audit we noted improvements in the areas of conducting physical inventories and reconciling property records to the financial records. However, we identified continuing weaknesses in several areas. Specifically, the FBI failed to adequately: (1) maintain records on how many of its laptop computers were authorized to process classified information; (2) improve its documentation of the disposal of excess laptop computers and hard drives to ensure that all sensitive or classified information had been sanitized prior to disposal; (3) report weapon and laptop losses to the DOJ; (4) improve the process to ensure that property is recovered from employees before they leave FBI service; and (5) adhere to its policy on property storage.

[20] When we began our follow-up audit, there were over 10,000 laptops that were not specifically assigned to FBI personnel. All laptop computers are required to be charged out in the PMA and assigned to individuals in an effort to strengthen accountability and minimize unexplained losses. We found that as of March 2006, 37 percent of the FBI's laptop computers had not been recorded as being assigned to individuals. However, after we inquired about this issue in March 2006, the FBI made a significant effort to assign the laptop computers to specific individuals. Therefore, as of May 2006 less than 1 percent of the FBI's laptop computers were not assigned to individuals.

Physical Inventories

The FBI's regulations require an annual inventory of all sensitive capitalized assets and sensitive property items, which include weapons and laptop computers. The FBI is also required to conduct a full inventory of all property and equipment every 2 years.

During our follow-up audit, we reviewed FBI-wide inventory reports for the years 2003 through 2005. We noted that the FBI had completed biennial inventories of all accountable property and annual inventories of sensitive items, including weapons and laptop computers.

Reconciling Property Records to the Financial System

In our 2002 audit report, we determined that the FBI's financial system was not fully integrated with the Property Management Application. 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. We recommended that the FBI implement a policy requiring that property records be reconciled with financial records to ensure the completeness of the FBI's property records.

In response to this recommendation, the FBI stated that the Asset Management Unit and Contract Unit would coordinate to ensure that the Property Management Application was updated manually to include purchases of non-capitalized property, including weapons and laptops. Further, FBI divisions were instructed to generate and review on-order reports on a monthly basis to ensure that newly purchased property was added to the PMA.[21] In addition, the Asset Management Unit generated delinquent on-order reports and distributed them to the appropriate APOs for follow-up.

In our follow-up review, we determined that the FBI's financial system was still not fully integrated with the PMA, although all divisions currently have the capability to generate an on-order report. In addition, we verified that FBI divisions have been instructed to generate the report on a monthly basis to review newly purchased property that should be placed in the PMA. We also noted that the Asset Management Unit generates delinquent on-order reports and distributes all copies to the APOs for follow-up.

As a result of our follow-up review, we concluded that the FBI had implemented a sufficient policy requiring that property records be reconciled to the financial records to ensure the property records are complete.

[21] An on-order report reflects capitalized and non-capitalized property valued at $1,000 and above, and also sensitive property that should be placed in the PMA.

Accuracy and Completeness of Property Records in the PMA

In our 2002 audit, we performed two tests to determine the accuracy and completeness of the PMA. We judgmentally selected weapons and laptop computers from the PMA and physically verified their existence. We also judgmentally selected items that were physically located at selected field and headquarters offices and traced them to the PMA. In our 2002 audit the FBI was able to provide all weapons and laptop computers for our physical verification.

During our follow-up audit, we performed the same two tests to determine the accuracy and completeness of the PMA. First, we selected a random sample of 497 weapons and 477 laptop computers from the PMA and physically verified their existence. We evaluated property records and property management activities at FBI headquarters and offices in New York, New York; Los Angeles, California; Washington, D.C.; Chicago, Illinois; and Miami, Florida.[22] The FBI was able to provide all weapons and laptop computers for our physical verification, except for one weapon and two laptop computers assigned to FBI headquarters, for which the FBI provided confirmations of their existence.

We also tested the completeness of the property records by selecting a sample of 10 weapons and 10 laptop computers held at each of the field offices. We reviewed and traced them to the PMA and found no discrepancies.

Reporting Requirements for Laptop Computers Containing NSI

The DOJ's Office of the Chief Information Officer (CIO) requires the FBI to report the number of laptop computers it has authorized for processing classified information. During our follow-up audit, we requested but did not receive from the FBI or the DOJ CIO these required reports. FBI officials told us that they did not keep records related to the classification level of each laptop, and the DOJ CIO confirmed that the FBI had not submitted the report. Further, the DOJ Office of the CIO stated that it had requested that the FBI submit the report by June 4, 2006. When we contacted DOJ CIO on June 12, 2006, we determined that the FBI had not submitted the report.

In September 2006, the FBI provided us with a list containing classification levels for 1,925 of its approximately 25,000 laptop computers. According to the FBI, it deployed a software application in June 2006 to register all FBI electronic devices. The application requires users to register their assigned devices and to indicate the security classification of each

[22] The universe of weapons and laptop computers for each audited location and details of our sample, by property type, location, and type of test, appear in Appendix II.

device. FBI officials told us that they are in the process of completing the registration for the remaining 23,000 laptops.

Reporting Losses to DOJ

DOJ Semiannual Theft Reports

DOJ regulations require all components to submit to DOJ semiannual reports summarizing loss of government property that occurred in the preceding six months from January 1 and July 1 of each year. In our 2002 audit, we found that four of the five semiannual reports submitted by the FBI to the DOJ were submitted late, ranging from 6 to 106 days. In addition, the semiannual reports were inaccurate with respect to the number of weapon and laptop losses. We recommended that the FBI submit complete, accurate, and timely semiannual reports to the DOJ Security Officer. The FBI agreed with our recommendation.

However, in this follow-up audit, we found that one required report was not submitted at all, and all of the submitted reports were incomplete and inaccurate. For example, in its semiannual reports the FBI reported to the DOJ only 106 lost or stolen weapons compared to the 160 we found in our review, and 97 laptop computer losses compared to the 160 we found in our review. Further, only three of the seven laptop computers that were identified as having sensitive or classified information were reported to DOJ. The remaining four were not reported in the semiannual reports. In our judgment, the FBI has not adequately improved its procedures relating to timely and accurate semiannual reports of losses of government property.

DOJCERT

DOJ regulations also require all components to submit immediate reports summarizing computer security incidents involving the loss of both classified and unclassified systems to the Department of Justice Computer Emergency Response Team (DOJCERT). The DOJCERT assists in handling computer security incidents throughout DOJ.[23]

We contacted DOJCERT officials to determine if the FBI submitted the required incident reports for the 160 laptop computers that were identified as lost or stolen during our review period. We determined that of the 160 laptops that FBI reported as lost or stolen during the 44-month review period, it had only submitted one incident report to the DOJCERT. This

[23] According to the DOJCERT, computer security incidents are any unexpected, unplanned event that could have a negative impact on IT resources. Computer security incidents can include the loss of both classified and unclassified systems, unauthorized removal of computer equipment, and exploited weaknesses in a computer system that allows unauthorized access to password files.

incident report contained information regarding a laptop computer that contained sensitive information reported stolen from the FBI's Criminal Justice Information Services (CJIS) Division on June 24, 2005. The FBI did not report any of the other lost or stolen laptop computers to the DOJCERT, including the other 9 that the FBI believed contained sensitive or classified information.

We asked the FBI's Enterprise Security Operations Center (ESOC), the unit responsible for submitting incident reports summarizing computer losses, why only one incident was reported to the DOJCERT. In response, the ESOC officials stated that prior to an OMB memorandum, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* dated July 12, 2006, the FBI was only responsible for submitting incidents to the DOJCERT that pertained to the loss of Personally Identifiable Information. However, as stated previously, as a result of our review we identified a stolen laptop containing the names, addresses and phone numbers of FBI personnel that was not reported to the DOJCERT. Further DOJCERT officials confirmed that the reporting of incidents involving the loss of both classified and unclassified systems to the DOJCERT has been a requirement since the inception of the United States Computer Emergency Readiness Team (US-CERT) in 2003.[24]

Disposal of Weapons and Laptop Computers

In our 2002 audit report, we found that the documentation for laptop disposals did not identify whether hard drives were properly destroyed and disposed of and were free of classified information. We recommended that the FBI improve its documentation of outdated, damaged, or excess laptop computers and hard drives that have been discarded.

To determine if the FBI improved its documentation of laptop disposals, we requested the disposal records for a sample of excessed hard drives at each of the five field offices we visited during our follow-up audit. We found that the FBI field offices did not retain documentation indicating whether it removed hard drives from excessed laptop computers and sent them to FBI headquarters for disposal. Officials at several of the field offices told us that they believed the proper procedure had been followed for laptop disposal, but they could not provide evidence of this. Therefore, we could not confirm whether the FBI was ensuring that the laptops it disposed of were properly sanitized of sensitive or classified information.

[24] The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

Exit Procedures for Departing Employees

During our 2002 audit, we found indications that the FBI was not recovering all issued weapons and laptops from employees prior to their departure from the organization. We recommended that the FBI strengthen procedures to ensure that departing employees return all property that had been issued to them or reimburse the government for the cost of such property. In response to the recommendation, the FBI revised its policy and distributed an electronic communication to all employees who were leaving, notifying them that they could be held accountable for lost or stolen FBI property.

During our follow-up review, we judgmentally selected the files of 50 former employees and reviewed the corresponding Forms FD-281 and FD-193s for both weapons and laptops issued to each of the 50 employees.[25] The FBI could provide only 19 Forms FD-281 for weapons and laptop computers, and only 32 of the required 50 Forms FD-193. Based on our overall review of the 160 weapon losses, we concluded that four of the lost or stolen weapons were the result of an agent leaving the FBI and not returning their weapon. In our judgment, the FBI has not sufficiently strengthened its exit processing for departing employees.

Conclusions and Recommendations

The FBI has made progress in decreasing the rate of loss for weapons and laptops, although it still has a significant number of FBI weapons and laptops lost or stolen each year. Moreover, several of the missing laptops contained sensitive information, and the FBI's documentation does not indicate how many of the other missing laptops contained sensitive or classified information.

Our audit also found that the FBI has not taken sufficient corrective action on several recommendations contained in our 2002 audit report. We determined that FBI is not reporting lost or stolen weapons and laptops as required. The FBI also is not consistently entering losses of weapons into NCIC or ensuring that all departing employees turn in their weapons.

[25] The Receipt for Government Property form (Form FD-281) is used for documenting both the receipt and return of government property. The Report of Exit and Separation form (Form FD-193) documents a variety of actions that must be completed upon an employee's departure.

Our audit report contains 13 recommendations to the FBI related to ensuring compliance with FBI policies and reporting requirements, as well as ensuring that weapon and laptop losses are appropriately reported and investigated. For example, the FBI needs to ensure that employees report the contents of lost laptop computers on the FD-500, that the FBI timely and accurately reports losses of laptops to DOJ, that all lost or stolen weapons are entered into NCIC, and that that all departing employees return FBI property.

TABLE OF CONTENTS

INTRODUCTION

In 2001, the Attorney General requested that the Office of the Inspector General (OIG) conduct audits of the controls over weapons and laptop computers throughout the Department of Justice (DOJ) in response to concerns about the DOJ's accountability for such property. Therefore, the OIG conducted separate audits of the controls over weapons and laptop computers at the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Federal Bureau of Prisons (BOP), and the United States Marshals Service (USMS).[26] The OIG issued separate reports on each component and an overall report summarizing the results from each audit.

In August 2002, we issued our report on the FBI's control over weapons and laptop computers.[27] Our report disclosed significant losses of weapons and laptop computers and examined the inadequacy of the FBI's response to these losses. The report concluded that the FBI's procedures to prevent the loss of inventory were not adequate. Specifically, we found that the FBI:

- identified 212 functional weapons, 142 inoperable training weapons, and 317 laptop computers as lost, missing, or stolen for our 28 month review period.

- did not always report missing items to the DOJ or enter lost and stolen weapons and laptop computers into the National Crime Information Center (NCIC) database.[28]

- did not have policies requiring the reporting of lost or stolen laptop computers to its Office of Professional Responsibility (OPR), and was not investigating these incidents in a timely manner.

---

[26] The OIG also conducted a property audit, including weapons and laptop computers, of the Immigration and Naturalization Service (INS), but the report was issued prior to the Attorney General's request. Department of Justice, Office of the Inspector General. Audit Report 01-09, *Immigration and Naturalization Service Management of Property*, March 2001. The INS was transferred to the Department of Homeland Security in 2003.

[27] Department of Justice, Office of the Inspector General. Audit Report 02-27, *The Federal Bureau of Investigation's Control over Weapons and Laptop Computers*, August 2002.

[28] NCIC is a computerized index of criminal justice information, including criminal history information, fugitives, stolen property, and missing persons, that is available to federal, state, and local law enforcement and other criminal justice agencies.

- had not established deadlines for reporting losses.
- was not conducting physical inventories as required.
- was not reconciling its property records to its financial records.
- was not always ensuring that exit procedures were followed for separating employees to ensure that they returned all issued property.
- could not provide documentation to establish whether excessed laptop computers were properly disposed of as required.

To address these deficiencies, we recommended that the FBI: (1) revise its policy for protecting equipment from loss and for disciplining employees when they do not follow FBI policy; (2) establish deadlines for reporting, documenting, and investigating losses; (3) ensure it conducts periodic inventories; (4) reconcile the property records to the financial records; (5) ensure that departing employees return all property that was entrusted to them; and (6) improve documentation showing that excess property had been properly disposed. The FBI agreed with these recommendations and outlined a plan for taking corrective action.

Background

As of March 31, 2006, the FBI employed 12,515 Special Agents and 17,915 support personnel located in 56 field offices across the United States; the Training Academy at Quantico, Virginia; over 50 international offices; and FBI headquarters in Washington, D.C. In December 2005, the FBI reported that 52,263 weapons and 26,166 laptop computers were assigned to FBI offices and employees located around the country and abroad.[29]

The FBI's inventory of weapons includes semi-automatic pistols, rifles, carbines, shotguns, tear-gas guns, and submachine guns. The term "weapons" includes not only those used operationally, but also training weapons that the FBI refers to as "red handles," which are incapable of firing live ammunition. In this report, we treat functional weapons and inoperable training weapons separately.[30]

[29] See Appendix VIII for an analysis of FBI assigned weapons and laptops.

[30] Training weapons include those that fire only blanks or paint-marking munitions. The FBI's Firearms Training Unit (FTU) considers it unlikely that anyone would convert a training weapon to a functional weapon because the conversion would be more expensive than the cost of a new functional weapon. Further, the conversion would require the

Laptop computers are assigned to most FBI special agents and many other FBI employees. Among other things, agents use laptops to prepare investigative reports, access various law enforcement databases, and support electronic surveillance activities.

Property Management Application System

The Office of Management and Budget Circular A-123 requires federal agencies to: (1) establish a management control system that provides reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation; and (2) ensure that transactions are promptly recorded, properly classified, and accounted for in order to prepare timely accounts and reliable financial and other reports.[31] The Justice Property Management Regulations require that DOJ components issue detailed operating procedures to protect federal property against fraud, waste, and abuse.[32]

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

- *Accountable Property Manual,*
- *Manual of Investigative Operations and Guidelines,* 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.

The FBI's Accountable Property Manual defines the three principal categories of property as:

- **Capitalized Property** which has an initial acquisition value of $25,000 or more, and that must be posted to the general ledger and accounted for on the annual financial statements;

---

services of a skilled gunsmith and parts that are available only from the manufacturer or from a licensed gun dealer.

[31] Office of Management and Budget. "Management's Responsibility for Internal Control," Circular A-123, December 21, 2004.

[32] Department of Justice Order (DOJ Order) 2400.3, dated August 6, 1998.

- **Accountable Property** which, because of its value or nature, must be accounted for on an individual basis in the Property Management Application (PMA). The PMA is an automated system that accounts for all property that the FBI acquires, transfers, and retires.[33] The FBI treats both weapons and laptop computers as accountable (non-expendable) property.

- **Expendable Property** such as supplies and equipment that are normally consumed within a 1-year period.[34]

Designated Property Management Employees

According to the *Accountable Property Manual*, the Chief of the Property Procurement and Management Section, located within the Finance Division, is the Property Management Officer (PMO) for the FBI. The PMO is responsible for administering the FBI's Property Management Program and ensuring that controls are adequate for accounting for FBI property.

Within each field office or headquarters unit, the Special Agent in Charge or an Assistant Director is designated as the Accountable Property Officer (APO). An APO is responsible for coordinating property management activities and providing leadership and guidance to ensure effective internal control procedures are in compliance with FBI requirements. An APO also ensures property records are created, and the property management program within their office is in compliance with the FBI's Accountable Property Manual and MAOP.

To assist them in the performance of their duties, APOs may designate one or more Property Custodians or Supply Technicians, depending on the size and complexity of an office. In addition, the Accountable Property Manual states that FBI employees are responsible for safeguarding property within their control.

According to the MAOP, the loss, misplacement, theft or destruction of government property issued to any employee must be reported to his or her superior within 5 calendar days of the loss, misplacement, theft or destruction. The division or field office must report the loss, misplacement, theft or destruction on a Form FD-500, Report of Lost or Stolen Property

[33] The PMA uses a variety of data fields to identify each item, including a barcode number assigned by the FBI, serial number, cost center code for the office where the item is located, description of the item, and other necessary information.

[34] The FBI Accountable Property Manual, Introduction and Section 2, paragraphs 2-4 and 2-22.

form, to the Asset Management Unit, Property Procurement and Management Section, Finance Division within 10 calendar days. The APO for the division or field office must sign the Form FD-500. In addition, the Security Division is required to be notified when laptop computers have been reported lost or stolen.

Once a loss is reported to the Asset Management Unit, the Property Management Officer is responsible for ensuring that all necessary information is obtained and it is forwarded to the proper headquarters units responsible for investigating and reviewing the losses. Also the PMO is responsible for updating the PMA to reflect the property loss.

Once a laptop loss is reported to the Security Division, the Security Compliance Unit is responsible for initiating an inquiry to the respective field office regarding the loss to assess the contents of the laptop, whether or not the laptop contained sensitive or classified information, and if National Security Information has been compromised.

Automated System – The FBI employs the automated PMA "to properly and accurately account for all property that the FBI acquires, transfers, and retires."[35] Information contained in the PMA includes the description, serial number, barcode number assigned by the FBI, code for the office where the item is located, and other necessary information. The PMA can produce a "Property Charged Out" report for any active or separated employee showing all accountable property that had been, or is still, assigned to that employee.

The FBI's Firearms Training Unit supplements the PMA with an index card for each weapon in its inventory. Like the PMA, the index cards include the serial number, barcode number (if applied to the weapon), individual or office to whom the property is assigned, and the final disposition of the weapon. The index card also includes details of any repairs that had been made to the weapons.

Audit Approach

The FBI had the greatest number of losses, as well as the most significant deficiencies in controls, of all the DOJ components we reviewed in our 2002 audits of controls over weapons and laptops.[36] We conducted this follow-up audit to assess the FBI's progress in addressing the deficiencies we

[35] Accountable Property Manual, Section 2, Paragraph 2-38.

[36] The problems in the INS were comparable, but INS functions were transferred to the Department of Homeland Security in 2003.

identified related to its control over weapons and laptops.[37] Our follow-up audit focused on a 44-month review period (February 1, 2002, through September 30, 2005).

In this follow-up audit, we interviewed FBI officials, reviewed documents, and tested controls at the FBI Headquarters in Washington, D.C., the Training Academy at Quantico, Virginia, and field offices in Chicago, Illinois; Los Angeles, California; Miami, Florida; New York, New York; and Washington, D.C. Fifty two percent of all weapons and 54 percent of all laptop computers were assigned to these offices.

Our audit examined actions taken in response to the identification of lost or stolen weapons and laptop computers. We reviewed the FBI's current procedures for responding to reports of missing weapons and laptop computers to determine whether losses are being reported in accordance with prior recommendations. We also queried NCIC and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Tracing Center to identify lost or stolen FBI weapons that were recovered or used in the commission of a crime.[38] For laptop computers, we queried NCIC to identify recovered property and assessed whether national security or investigative information may have been compromised. We address these issues in Finding I.

In addition, we reviewed the FBI's internal controls over accountable property, exit procedures for departing employees, and disposal of property. Our assessment included physically verifying a sample of weapons and laptop computers. We also tested the accuracy and completeness of the property records. The results of these analyses are presented in Finding II.

[37] Appendix I contains more information on the current audit's objectives, scope, and methodology.

[38] The ATF National Tracing Center tracks the history of recovered crime guns for federal, state, local, and international law enforcement agencies.

FINDINGS AND RECOMMENDATIONS

I. FBI'S RESPONSE TO WEAPON AND LAPTOP LOSSES

Our 2002 audit found that over a 28-month period the FBI lost or had stolen 354 weapons and 317 laptop computers. Our follow-up audit found that over a 44-month period the FBI lost or had stolen 160 weapons and 160 laptop computers, including 10 that contained sensitive or classified information. We noted improvements in the rate of loss for each category of equipment except for stolen laptop computers, which increased slightly. However, we found that the FBI did not know whether many of the laptop computers that were reported lost or stolen contained sensitive or classified information. We also found that the FBI has not taken adequate corrective action on several recommendations outlined in the 2002 audit report. As a result of our 2002 audit, the FBI established deadlines for reporting lost and stolen weapons and laptop computers, entering those losses into NCIC, and referring the losses for investigation. But this follow-up audit determined that the FBI did not consistently follow those procedures.

Rate of Weapon and Laptop Losses

To determine whether the FBI has made progress in reducing the number of lost and stolen weapons and laptop computers, we first compared the rate of loss from our 2002 audit to this follow-up audit. We found that, except for stolen laptop computers, the rate of loss decreased, as detailed in the following table.[39]

[39] Because the audit periods were different lengths, we analyzed the rate of loss on a monthly basis.

MISSING WEAPONS AND LAPTOP COMPUTERS
2002 AUDIT VS. FOLLOW-UP AUDIT[40]

Category	Number of Lost or Stolen Items Reported		Losses Reported Per Month	
	2002 Audit (28 Month Period)	Follow-up Audit (44 Month Period)	2002 Audit	Follow-up Audit
Lost Functional Weapons	107	48	3.82	1.09
Stolen Functional Weapons	105	94	3.75	2.14
Lost Training Weapons	142	18	5.07	0.41
Stolen Training Weapons	0	0	0	0
Total Lost or Stolen Weapons	***354***	***160[41]***		
Lost Laptop Computers	300	116	10.71	2.64
Stolen Laptop Computers	17	44	0.61	1.00
Total Lost or Stolen Laptops	***317***	***160***		

Source: OIG analysis of FBI data

We noted improvements in the rate of loss for each category of equipment except for stolen laptop computers, which increased slightly. However, despite the FBI's progress in decreasing the rate of loss for weapons and laptops, the FBI still reported 160 weapons and laptops that were lost or stolen. We recognize that in an organization the size of the FBI, some weapons and laptops will inevitably be stolen or go missing. However,

[40] Our review period for the 2002 audit covered 28 months, from October 1, 1999, to January 31, 2002. Our review period for our follow-up audit covered 44 months, from February 1, 2002, to September 30, 2005.

[41] The FBI objected to the inclusion of 43 of these 160 weapons because while they were reported as lost or stolen during our 44 month follow-up period, the loss actually occurred before our follow-up period. We did not delete these weapons from the table because: (1) the losses were not categorized as such in the FBI's official property management system until after the beginning of our follow-up period, (2) our approach in the follow-up audit was consistent with our approach in the 2002 audit, which also included weapons that were reported as lost or stolen during our review period, (3) none of these 43 weapons were included in the 354 lost or stolen weapons reported in the 2002 audit, (4) to delete them would give the appearance that the FBI had 43 fewer lost or stolen weapons than was actually the case.

it is important that the FBI take appropriate steps to minimize these losses. When losses occur, the FBI must timely report the loss, be able to identify the contents of lost laptops, and determine whether the laptop is encrypted. In addition, the FBI must investigate these losses and thefts, enter required data into the National Crime Information Center (NCIC), and report the losses to DOJ as required.

We found that the FBI has not taken adequate corrective action on several recommendations outlined in our 2002 audit report. Further, the FBI did not determine for all of its lost or stolen laptop computers whether they contained sensitive or national security information. All users of FBI laptop computers had access to sensitive information and the equipment was authorized for processing classified information up to the Secret level. The FBI does not know which of its laptop computers actually contained classified information.[42]

In the following sections, we report on: (1) the circumstances surrounding each FBI weapon and laptop loss, (2) the contents of the lost or stolen laptop computers, (3) the FBI's internal and external loss-reporting process, including entry into NCIC, and (4) the FBI's efforts to investigate losses.

Weapons Losses

In our 2002 audit, we noted that in many instances the loss of weapons was preventable because employees either did not adequately safeguard property that had been assigned to them or follow FBI policies. Our 2002 audit also found five instances in which lost or stolen FBI weapons were subsequently used in the commission of a crime.

As shown in the table below, for the current review period 94 of 160 (59 percent) missing weapons were stolen from FBI vehicles, private vehicles, or employee residences. These lost and stolen weapons included handguns, rifles, shotguns, and submachine guns. Pistols accounted for 133 of the 160 (83 percent) lost weapons.

[42] As we explain in Finding II, the FBI did not maintain records indicating which of its laptop computers were authorized to process National Security Information.

LOST AND STOLEN WEAPONS BY TYPE
FEBRUARY 1, 2002, THROUGH SEPTEMBER 30, 2005

	Pistol	Shotgun	Submachine Gun	Rifle	Total
Lost:					
Unexplained Loss	40	3	0	0	43
Miscellaneous [43]	23	0	0	0	23
Subtotal	***63***	***3***	***0***	***0***	***66***
Stolen:					
From FBI Vehicle	28	6	5	7	46
From Residence	11	0	0	0	11
From POV [44]	11	1	0	0	12
Other [45]	20	3	1	1	25
Subtotal	***70***	***10***	***6***	***8***	***94***
Total	**133**	**13**	**6**	**8**	**160**

Source: OIG analysis of FBI Forms FD-500 (Reports of Lost and Stolen Weapons)

Although our follow-up review of FBI files found instances where thefts occurred despite reasonable precautions taken by FBI employees, we also found examples of lost or stolen weapons that resulted from employees' carelessness or failure to follow FBI policy. Details of those losses are listed in Appendix III.

Laptop Computers Losses

In March 2001, the FBI Director issued a memorandum requiring that all losses of laptop computers be reported to OPR because, "the loss of a laptop with classified or sensitive information could be potentially more damaging to the FBI than a lost weapon."

The FBI also issued a memorandum dated November 1, 2002, outlining circumstances under which employees would be held accountable for the cost of the lost or stolen property. The memorandum stated that employees were responsible for securing property assigned to them and would be personally responsible for the value of any property that was lost, stolen, or not returned to the government.

[43] Includes 18 inoperable training weapons.

[44] Privately Owned Vehicle.

[45] These weapons were lost under a variety of circumstances. For example, one weapon was stolen from a rental car. Another was stolen from a Special Agent's desk drawer at a field office.

Similar to the reports of lost and stolen weapons, many laptop computer losses could have been avoided had employees been more careful or had followed FBI policies. Details of these losses are listed in Appendix IV.

As shown below, we were unable to determine the circumstances of the losses for 116 of 160 missing laptop computers (72 percent) because FBI documentation did not include a description of how the item was lost. Sixty-two of these laptops were identified as lost when the FBI conducted its biennial inventories. The remaining 44 laptop computers (28 percent) were stolen from vehicles and other locations.

LOST AND STOLEN LAPTOP COMPUTERS
BY LOSS TYPE
FEBRUARY 1, 2002, THROUGH SEPTEMBER 30, 2005

	Total
Lost:	
Unexplained Loss	116
Stolen:	
From FBI Vehicle	23
From Residence	4
Other [46]	17
Subtotal	***44***
Total	**160**

Source: OIG analysis of FBI Forms FD-500

Reporting Weapons and Laptop Computer Losses

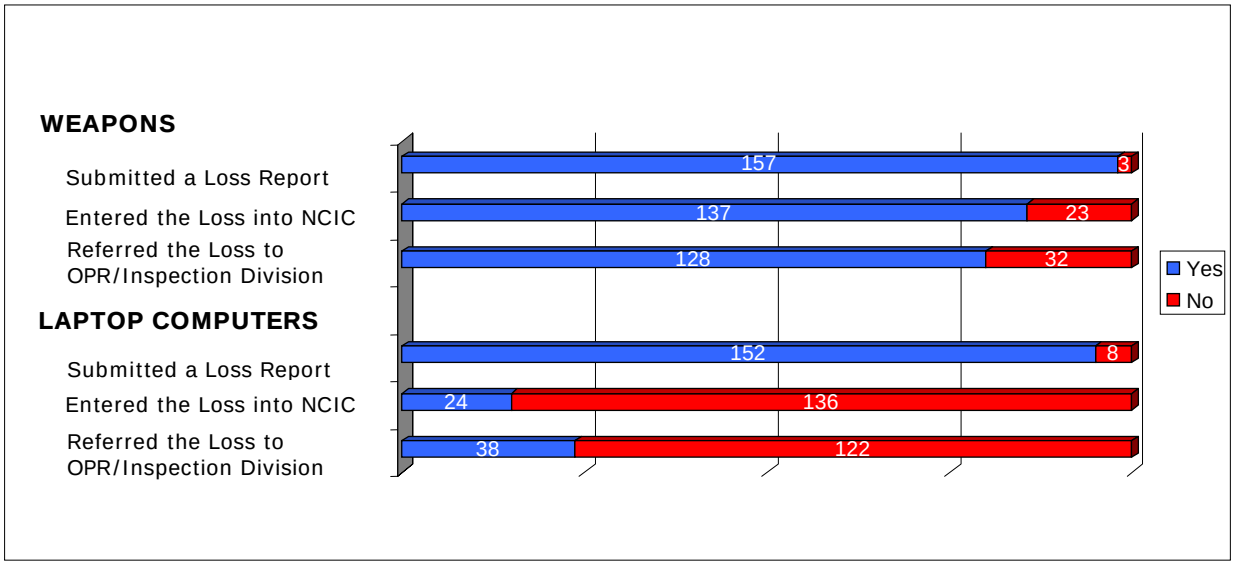
During our initial review in 2002, we found that the FBI did not specify deadlines for submitting the Report of Lost or Stolen Property form (Form FD-500) to report loss of property. As a result, we recommended that the FBI establish and adhere to firm deadlines to ensure that: (1) employees promptly report the loss or theft of FBI property to their supervisors; (2) supervisors report losses or thefts to headquarters units, including the Firearms Training Unit, OPR, the Asset Management Unit, and the Security Division; (3) OPR initiates and completes an investigation into the loss; and (4) information from the Form FD-500 is entered into NCIC.

[46] These laptop computers were stolen under a variety of circumstances. For example, one laptop was stolen from a hotel room. Another was stolen from a Special Agent's privately owned vehicle.

In response, the FBI revised its policy on August 14, 2002, requiring that employees report lost or stolen weapons and laptop computers to their division or field office within 5 days after discovery of the loss. Division or field offices, in turn, are required to submit a Form FD-500 to the Asset Management Unit within 10 days of the loss. All losses of weapons and laptop computers are required to be entered into NCIC and forwarded to the Inspection Division for investigation.[47] Laptop computer losses are required to be reported to the Security Division.

We reviewed the reporting actions that the FBI took in response to the lost or stolen weapons and laptop computers by examining the Forms FD-500. We assessed whether the loss was reported to the Asset Management Unit, entered into NCIC, referred for investigation, and if a laptop, reported to the Security Division. The table below categorizes our findings.

FBI REPORTS OF THE LOSS OR THEFT OF WEAPONS AND LAPTOP COMPUTERS FEBRUARY 1, 2002, THROUGH SEPTEMBER 30, 2005



Source: OIG analysis of FBI data

Of the 160 missing weapons, the FBI was able to provide Forms FD-500 for 157 weapons. The remaining three weapons were missing the required forms. We asked the Asset Management Unit officials about the missing forms and were told that they existed at one point but at the time of

[47] Since the issuance of our initial audit report in 2002, the FBI reorganized OPR and the Inspection Division. In February 2004, the FBI transferred the responsibility for investigations of alleged employee misconduct from OPR to the Inspection Division. The OPR continues to be responsible for adjudicating disciplinary matters.

our review they could not be found. Despite not having the Forms FD-500, the Asset Management Unit retained minimal information regarding the weapon losses, such as the serial numbers, by recording that information onto a list that was provided to us during our follow-up review. Of the 157 for which there was a Form FD-500, we found:

- 18 were reported using an outdated Form FD-500.[48] The old form did not capture critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 92 weapon losses were reported on the new Form FD-500. However, 51 of the 92 new Forms FD-500 were incomplete because the individual preparing the form did not enter critical information such as the date of loss, NCIC entry, and whether the loss was referred to OPR for investigation.

- 54 were reported late—more than the required 10 days—thus possibly delaying timely investigation regarding the circumstances of the loss. See Appendix V for details on the number of days losses were reported late.

Of the 160 missing laptop computers, the FBI was able to provide Forms FD-500 for 152 laptops, while 8 laptops were missing the required form. Similarly, we asked the Asset Management Unit officials about the missing forms and were told that they existed at one point but at the time of our review, they could not be found. Despite not having the Forms FD-500, the Asset Management Unit retained minimal information regarding the laptop losses, such as barcodes and serial numbers, by recording the information onto a list that was provided to us during our follow-up review. Of the 152 that were reported using a Form FD-500, we found:

- 24 were reported using an outdated Form FD-500.[49] The old form did not capture critical information such as the date of loss, NCIC entry, and whether OPR was notified.

[48] The Form FD-500 was updated on July 24, 2002, to include new fields. An additional 47 FD-500's submitted prior to July 24, 2002 did not contain critical information such as the date of loss, NCIC entry, and whether OPR was notified.

[49] An additional 21 Forms FD-500 that were submitted prior to July 24, 2002 did not contain critical information such as the date of loss, NCIC entry, and whether OPR was notified.

- 107 laptop losses were reported on the new Form FD-500. However, 82 of the 107 new Forms FD-500 were incomplete because the individual preparing the form did not enter critical information such as the date of loss, NCIC entry, and whether the loss was referred to the Security Division as well as OPR for investigation.

- 38 were reported late—more than the required 10 days—thus possibly delaying timely investigation regarding the circumstances of the loss. See Appendix VI for details on the number of days losses were reported late.

Regarding the reporting process for both weapons and laptop computers, Asset Management Unit officials explained that the field offices are responsible for submitting complete, accurate, and timely Forms FD-500. According to these officials, the Asset Management Unit's responsibility is essentially to ensure that property is accurately tracked in PMA. However, this understanding is contrary to the duties and responsibilities that have been assigned to the PMO in the Accountable Property Manual. The Accountable Property Manual states that the PMO is responsible for the overall administration, coordination and control of the FBI's Property Management Program. For a comprehensive listing of the lost and stolen weapons and laptops, see Appendices V and VI.

Thus, although the FBI strengthened its policy for reporting lost or stolen weapons and laptop computers by revising the Form FD-500 and establishing a new 10 day policy for reporting losses, the FBI did not ensure that its staff consistently used the revised form or reported the loss within 10 days, as required. We recommend that the FBI ensure that its staff prepare complete and accurate loss reports using the latest version of the Form FD-500 and submit those reports to the appropriate offices in a timely manner.

Contents of Lost or Stolen Laptop Computers

Our review of the 152 Forms FD-500 for lost and stolen laptops revealed that 101 were identified as *not* containing sensitive or classified information, 43 were not marked as either containing or not containing sensitive or classified information, and 8 were marked as containing

sensitive or classified information.[50] We asked the Security Division for any information that it had on the 160 laptop losses. We were provided limited information on only 12 laptop losses that the Security Division reviewed. Two of the 12 laptop losses that the Security Division reviewed were initially part of the 101 that were identified on the Forms FD-500 as not containing sensitive or classified information. The Security Division determined that these two laptop computers did contain sensitive, but unclassified information. Therefore, we added these two laptop losses to the eight that were identified on the Forms FD-500 as containing sensitive or classified information. Details related to the 10 laptops are provided in the table below.

[50] In addition to the 43 laptop losses for which the Forms FD-500 were not marked to indicate whether the laptops contained or did not contain sensitive or classified information, there were 8 laptop losses for which the Property Management Unit did not retain the Forms FD-500 and had no information on whether these laptops contained or did not contain sensitive or classified information. Therefore, we combined these 8 laptop losses to the 43 and discuss the FBI's response to these losses in more detail later in our report in the 51 Laptop Losses section.

DETAIL ON LAPTOP LOSSES
CONTAINING SENSITIVE OR CLASSIFIED INFORMATION

No.	Date of Loss	Office Reporting Loss	Type of Loss	Encrypted?	Nature of Contents
1	07/12/02	Boston Field Office	Stolen	Yes	Software for creating identification badges.[51]
2	09/02/02	Indianapolis Field Office	Lost	Unknown	Unknown
3	09/24/02	New Orleans Field Office	Stolen	Unknown	Used to process surveillance-related electronic digital imaging.
4	07/15/03	Phoenix Field Office	Lost	Unknown	Unknown
5	03/11/04	Security Division	Stolen	Yes	System security plan for an electronic access control system.
6	05/19/04	Washington Field Office	Lost	Unknown	Unknown
7[52]	05/06/05	Security Division	Lost	Unknown	Unknown - SCU determined contents to be sensitive, but unclassified.
8[53]	06/24/05	CJIS Division	Stolen	Yes	Unknown - SCU determined contents to be sensitive, but unclassified.
9[51]	08/21/05	San Diego Field Office	Stolen	Unknown	Unknown - SCU determined contents to be sensitive, but unclassified.
10	Unknown (approx. 07/02)	Quantico Laboratory Division	Stolen	Unknown	Names, addresses, and telephone numbers of FBI personnel.

Source: FBI Forms FD-500

As previously stated, 8 of the 10 laptop losses were identified on the Forms FD-500 as containing sensitive or classified information the Forms FD-500 for these eight laptop losses did not specifically make a distinction as to whether the sensitive information included National Security Information (NSI). We asked Asset Management Unit and Security Division officials whether they could identify if any of the eight laptops did in fact contain

[51] The Form FD-500 for the laptop loss from the Boston Field Office was marked to indicate that it did not contain sensitive/classified information *and* that it did contain sensitive/classified information. Because both answers are mutually exclusive and the description of the contents was consistent to information that can be considered sensitive/classified, we considered this laptop as containing sensitive/classified information.

[52] The Forms FD-500 for these laptop losses indicated that the corresponding laptops did not contain sensitive or classified information. However, according to subsequent information that we obtained from the Security Division's Security Compliance Unit (SCU), the SCU concluded that the laptops contained sensitive but unclassified information.

[53] The laptop computer that was reported as being stolen from the Criminal Justice Information Services (CJIS) Division was also the only laptop computer reported to DOJCERT.

National Security Information. The Security Division provided us information to indicate that the laptop loss reported by the CJIS Division on June 24, 2005, contained sensitive but unclassified information.[54] FBI officials did not know whether the remaining seven laptops that were identified as sensitive actually contained National Security Information.[55]

According to OPR and Investigation Division records, the FBI investigated 6 of the 10 laptops losses that were known to contain sensitive or classified information.[56] Of the six laptop losses that were investigated, one resulted in a 3-day suspension, two investigations were pending as of February 2006, and three resulted in no action taken against the employee. The FBI did not investigate the remaining four losses, including the laptop computers that contained personal identifying information of FBI personnel and software for creating identification badges.[57]

Similarly, we asked FBI Security Division officials if they conducted any type of review to determine the contents of the remaining seven laptop losses or to assess the potential damage to national security and the FBI's operations. Security Division officials stated that they are reviewing the Forms FD-500 and contacting the appropriate field offices to determine what kind of information was on the laptops. However, the Security Division officials informed us that because these losses occurred some time ago it is doubtful that the FBI would still have information about the content of the laptops.

---

[54] The CJIS Division laptop loss was also included as one of the 12 laptop losses that the Security Division reviewed. Of the 12 laptop losses that the Security Division examined, only 3 were identified as containing sensitive information. Five of the 12 laptops were determined by the Security Division to not contain sensitive or classified information and for the remaining 4; the Security Division did not know whether the laptops contained any sensitive or classified information.

[55] According to the FBI Security Handbook, 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. Classified information (National Security Information) 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. For further details on the classification levels of Classified National Security Information see Appendix XVII.

[56] OPR investigated laptop losses that are referred to in the above table as numbers 2, 3, 4, 8, and 9.

[57] See Appendix IV for a detailed description of the disciplinary action taken relating to the 160 FBI laptops that we identified in our follow-up audit as being lost or stolen.

51 Laptop Losses

The Forms FD-500 for 43 of the 51 laptop computers did not indicate whether the laptops contained sensitive or classified information, as required. The employee who completed the form did not check the box to indicate whether sensitive or classified information was or was not contained on the laptop, nor did the Accountable Property Officer or the Asset Management Unit complete that section of the form when it was submitted. An analysis of the 51 laptop computers is provided in the table below.[58]

ANALYSIS OF THE 51 LAPTOP COMPUTERS UNKNOWN TO HAVE SENSITIVE OR CLASSIFIED INFORMATION

Category	*Assigned To Employee*	*Unassigned*	*Total*
Unexplained Losses[59]	3	22	**25**
Loss Identified During Physical Inventory	5	16	**21**
Stolen from Vehicle	1	1	**2**
Stolen from FBI Office	0	1	**1**
Other	2	0	**2**
TOTAL	**11**	**40**	**51**

Source: FBI Forms FD-500

Seven of these 51 laptop computers were assigned to divisions within the FBI that handle some of the most sensitive information related to national security. Six of the 51 laptop computers were assigned to the Counterintelligence Division and 1 was assigned to the Counterterrorism Division. Yet, the FBI did not know the content of these computers or whether they contained sensitive or classified information.

Of these 51 laptops, 11 were referred to FBI's OPR/Inspection Division. Further, only two resulted in disciplinary action, including one letter of censure and one 3-day suspension. The documentation maintained at OPR did not contain the contents of these laptop computers.

Even though the FBI has a policy requiring that employees disclose the contents of lost or stolen laptops, this policy was not enforced. Most of the Forms FD-500 as detailed in Appendix IV did not have a description of the type of information contained on the laptop. This is a significant deficiency because some of these laptops may have contained classified or sensitive

[58] A more detailed analysis can be found in Appendix VIII.

[59] Eight of the 22 laptops that were *not* assigned to an employee and for which the loss was unexplained did not have Forms FD-500.

information such as personally identifiable information or investigative case files.[60] Without knowing the contents of these lost and stolen laptop computers, it is impossible for the FBI to know the extent of the damage these losses might have had on its operations or on national security.

Aside from reviewing the Forms FD-500 we asked FBI officials if they could determine the content of the 51 lost or stolen laptop computers and whether they contained sensitive or classified information. FBI officials explained that they did not maintain such information and therefore could not determine the content of the laptops or whether sensitive or classified information was contained on them. We asked FBI officials why they do not have this information. Security Division officials speculated that its SCU may not have been notified of the lost and stolen laptop computers and therefore would not have followed up in determining the contents of the lost or stolen laptops. However, our review of all 152 Forms FD-500 for lost and stolen laptop computers found that 64 were marked as having been referred to the Security Division.

We also asked FBI officials why they do not go to the respective field offices and divisions to obtain this information. As previously mentioned, Security Division officials stated that they are reviewing the Forms FD-500 and contacting the appropriate field offices to determine what kind of information was on the laptops.

FBI officials acknowledged to the OIG that there was a breakdown in obtaining the necessary information on the contents of the laptops that were lost or stolen. The FBI Security officials suggested that part of the cause may be attributed to the lack of a centralized unit within the FBI that could identify the contents of lost or stolen laptops or make sure that Forms FD-500 are complete and accurate. Further, the Security Division officials stated that they have since started tracking this type of information with the implementation of the Portable Electronic Device (PED) Application in June 2006.[61]

---

[60] Personally Identifiable Information is any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

[61] The FBI deployed the Portable Electronic Device (PED) Application to register all FBI electronic devices, including laptop computers. The PED Application draws baseline information from the FBI's PMA and requires users to register their assigned devices and to indicate the security classification of each device.

We believe that the FBI was lax in adhering to its own policies of reporting the contents of lost or stolen laptop computers. The FBI has to be more diligent in ensuring that it responds appropriately and aggressively to each laptop loss.

Entering Losses into NCIC

The NCIC is a computerized database of criminal justice information, such as stolen property, convicted offender registries, and an index of individuals incarcerated in the federal prison system. The NCIC system is generally regarded by law enforcement agencies as the primary method for tracking stolen or recovered firearms. Criminal justice agencies enter records into NCIC, which are then accessible to law enforcement agencies nationwide. Data regarding lost or stolen weapons and laptop computers should be promptly entered into NCIC. Failure to enter these items into NCIC could result in reducing the chances of recovering the weapon or laptop computer or identifying the weapon if it is used in the commission of a crime. In addition, FBI policy states that lost and stolen laptops are required to be entered into NCIC.

Our 2002 audit found that 14 of the 276 (5 percent) lost or stolen weapons had not been entered into NCIC. In our follow-up audit, we initially found no NCIC records for 23 of the 160 (14 percent) lost or stolen weapons and no NCIC record for 136 of the 160 (85 percent) lost or stolen laptops.[62] Of the 23 weapons and the 136 laptop computers, 11 weapons and 16 laptop computers had an NCIC number recorded on the corresponding Form FD-500, but we did not find a record in NCIC.[63] For a detailed listing of the weapons and laptops that were not found in NCIC see Appendices IX and X.

At our exit conference, FBI officials stated that 10 of the 23 weapons currently do not have a record in NCIC. Specifically, the FBI provided us information on the following:

- 6 weapons had active records, 3 of which occurred as a result of our review.

[62] In our prior audit, we did not determine whether lost or stolen laptop computers were entered into NCIC because there was no requirement at the time to enter lost or stolen laptop computers into the NCIC.

[63] An NCIC number is a unique record number that is assigned to an entry made into NCIC.

- 7 weapons were recovered and the record was purged from NCIC as a result.

- 3 weapons were not entered into NCIC.[64]

- 7 weapons were at one point entered into NCIC but later purged with no explanation.

We also queried NCIC to determine whether the lost and stolen weapons and laptop computers were recovered and, for the weapons, whether they were used in the commission of a crime. We identified no instances where law enforcement recovered any of the 160 lost or stolen weapons, or the 160 lost or stolen laptop computers. Therefore, we could not conclude whether any of the missing weapons were used in a crime. However, after completion of our fieldwork, the FBI reported to us that seven weapons had been recovered. Details of those weapons are listed in Appendix III.

Asset Management Unit officials explained that the field offices are responsible for entering lost or stolen weapons and laptop computers into NCIC. In our judgment, the FBI has improved its practice of entering lost or stolen property into NCIC. However, 85 percent of the lost or stolen laptop computers were not entered into NCIC, as required by FBI policy. The FBI should immediately enter into NCIC its lost or stolen weapons and laptop computers to ensure that any recovery of these property items will result in the FBI being notified.

Referring and Investigating Losses

Our 2002 audit found that losses of weapons and laptops were not regularly referred to OPR and that disciplinary action was not taken when individuals did not follow FBI policies concerning the handling of weapons and laptops. As a result, we recommended the FBI revise its policy and establish criteria for disciplining employees whose negligence resulted in the loss or theft of a weapon or laptop. In response to our recommendation, the FBI stated that it would require weapon and laptop losses to be referred to OPR.[65]

---

[64] Two weapons were claimed to have been found and therefore not entered into NCIC. However PMA continued to show these weapons as being lost or stolen and the FBI did not provide evidence that these weapons were found. One weapon was inoperable and disabled, although the FBI did not provide evidence of this.

[65] MAOP, Part 2, 6-7.5.

OPR's investigative responsibilities were transferred to the Inspection Division in February 2004. Specifically, the Inspection Division is responsible for investigating weapon and laptop losses while OPR is still responsible for adjudicating disciplinary matters.

Inspection Division officials told us that it delegates responsibility for conducting most investigations of lost or stolen weapons and laptops to the field office that reported the loss. If the results of the investigation warrant disciplinary action, the case is forwarded to OPR for adjudication. Inspection Division officials told us that in many cases the office that conducted the investigation found no evidence of misconduct and consequently no disciplinary action was taken.

REFERRALS AND INVESTIGATIONS OF WEAPON AND LAPTOP LOSSES

Category	Number of Lost or Stolen Items[66]	REFERRED			INVESTIGATED	
		Referred To OPR	Referred to Inspection Division	Not Referred	OPR/ID Investigated	Not Investigated
Lost Functional Weapons	48	19	16	13	12	36
Stolen Functional Weapons	94	50	35	9	58	36
Lost Training Weapons	18	8	0	10	0	18
Stolen Training Weapons	0	0	0	0	0	0
Total Lost or Stolen Weapons	**160**	**77**	**51**	**32**	**70**	**90**
Lost Laptop Computers	116	9	9	98	13	103
Stolen Laptop Computers	44	13	7	24	8	36
Total Lost or Stolen Laptops	**160**[67]	**22**	**16**	**122**	**21**	**139**

Source: OIG analysis of FBI data

[66] Of the 160 weapon losses, 11 were reported lost and 35 were reported stolen after February 2004. Of the 160 laptop losses, 42 were reported lost and 16 were reported stolen after February 2004.

[67] Of the 160 lost and stolen laptop computers, the FBI did not know whether 51 of these laptops had sensitive or classified information. Of the 51, 37 were lost, 6 were stolen, and the remaining 8 had no Forms FD-500 describing the loss as being either lost or stolen; therefore, we included the 8 in the lost category. Also, of the 51, 11 were referred to OPR/Inspection Division and from these 11 losses, 9 were investigated by OPR/Inspection Division; for the remaining two, OPR/Inspection Division lacked sufficient information to open an internal investigation.

The Inspection Division officials also stated that investigations were not pursued if preliminary information indicated that there was no negligence or misconduct on the part of the employee. For example, items identified as lost or stolen during a physical inventory were not considered by the Inspection Division to be indicative of negligence or misconduct. Details of our review are explained below.

Weapons Loss

The MAOP requires that each weapon loss must be referred to OPR. However we found that 32 weapons (20 percent) were not referred. Further, of the total 160 lost or stolen weapons OPR/Inspection Division opened an internal investigation into 70 (43 percent) of those losses. OPR/Inspection Division explained that it did not open an internal investigation for the remaining 90 losses for the following reasons:

- 22 losses did not receive requisite notification from field offices
- 58 had no evidence of employee misconduct that would warrant an internal investigation
- 10 were training weapons

Of the 70 weapon losses that resulted in an internal investigation the action taken was as follows:

- 43 resulted in suspensions of the responsible employees, ranging from 3 to 7 days,
- 17 resulted in no disciplinary action,
- 5 resulted in the employees receiving a Letter of Censure,
- 1 resulted in the employee being terminated, and
- 4 investigations were still pending.

We found it troubling that many of the weapon losses were not referred to OPR/Inspection Division for investigation even though the requirement in the MAOP clearly states that each weapon loss must be referred to OPR. As we previously mentioned, FBI officials told us that they do not investigate these losses because of insufficient information to indicate possible misconduct or negligence by an employee or the fact that the weapon was not specifically assigned to an employee.

Laptops Loss

The MAOP requires that each laptop loss must be referred to OPR. We found that 122 laptops (76 percent) were not referred. Further, of the total 160 lost or stolen laptops OPR/Inspection Division initiated an internal investigation into 21 (13 percent) of the losses. OPR/Inspection Division explained that it did not initiate an internal investigation for 139 losses because of the following reasons:

- 122 losses did not receive requisite notification from field offices
- 17 had no evidence of employee misconduct that would warrant an internal investigation

Of the 21 laptop losses that resulted in an internal investigation the action taken was as follows:

- 3 resulted in 3-day suspensions of the responsible employees,
- 11 resulted in no disciplinary action,
- 1 resulted in the employee receiving a Letter of Censure, and
- 6 investigations were still pending.

Similar to lost or stolen weapons, OPR/Inspection Division explained that cases are opened when there is sufficient evidence of an employee's misconduct, and that cases were not opened if the lost or stolen laptop was not assigned to specific FBI personnel.[68]

We found it troubling that the overwhelming majority of laptop losses were not referred to OPR/Inspection Division for investigation even though the requirement in the MAOP clearly states that each laptop computer loss must be referred to OPR. As we previously mentioned, FBI officials told us that they do not investigate losses because of insufficient information to

[68] When we began our follow-up audit, there were over 10,000 laptops that were not specifically assigned to FBI personnel. All laptop computers are required to be charged out in the PMA and assigned to individuals in an effort to strengthen accountability and minimize unexplained losses. We found that as of March 2006, 37 percent of the FBI's laptop computers had not been recorded as being assigned to individuals. However, after we inquired about this issue in March 2006, the FBI made a significant effort to assign the laptop computers to specific individuals. Therefore, as of May 2006 less than 1 percent of the FBI's laptop computers were not assigned to individuals.

indicate possible misconduct or negligence by an employee or the fact that the laptop was not specifically assigned to a person.

Based on the relatively low number of investigations initiated, the FBI, in our judgment, has not been as diligent as it should be in investigating weapon and laptop losses.

Lack of Centralized Oversight and Monitoring

According to the MAOP, the Forms FD-500 are to be forwarded to the attention of the FBI's PMO. The PMO is responsible for reviewing the details of lost and stolen items and requesting any additional information. In addition, the Accountable Property Manual states that the PMO's duties include the overall administration, coordination and control of the FBI's Property Management Program, including: (1) ensuring that adequate systems exist and are documented for accountability of property within the FBI: and (2) communicating and monitoring internal controls of the FBI for maintaining adequate property accountability.

The FBI's response to lost and stolen weapons and laptop computers demonstrated several weaknesses that resulted in inadequate reporting of weapon and laptop losses within the FBI. When reports were submitted, there did not appear to be any type of review at the Asset Management Unit to ensure that necessary information and documentation was received. Also, there did not appear to be consistent treatment by the divisions and field offices in notifying proper headquarters units, such as the Security Division and the Inspection Division. These deficiencies could have been avoided had the FBI provided more diligent oversight and monitoring in addressing the weapon and laptop losses.

The Asset Management Unit officials explained that its responsibility is to track property as opposed to ensuring that all of the proper procedures are followed for reporting lost and stolen items. However, we found this understanding to be different from what the FBI's Accountable Property Manual prescribes. We recommend that the FBI ensure that the Asset Management Unit provides oversight and monitoring for all weapon and laptop losses.

Conclusion

Our follow-up audit found decreases from our 2002 audit in the number of losses and the loss rates for weapons and laptops. However, while the number and rate of losses have declined overall, the amount is still

significant, and we found that the FBI has not taken adequate corrective action on several recommendations outlined in our 2002 audit report.

For example, we found that many of the forms that were used to report losses were incomplete, and critical information such as the date of the loss, NCIC entry, and whether OPR was notified of the loss was not provided by the divisions or field offices. Also, we found that the Asset Management Unit was not able to find all Forms FD-500 related to the lost and stolen weapons and laptop computers. The FBI was unable to determine what was on many of the laptops. Even when some of the lost or stolen laptops were identified as containing sensitive or classified information, the Security Division examined few of these losses to determine the damage that these losses may have had on the FBI's operations and national security.

Weapons and particularly laptop computers were not always being entered into NCIC. In addition, we found that weapon and laptop losses were not consistently referred to OPR/Inspection Division for investigation.

Recommendations

We recommend that the FBI:

1. Ensure that the Asset Management Unit maintains all Forms FD-500 with accompanying documentation and required information.

2. Ensure that the most current version of the Form FD-500 is used to report weapon and laptop losses.

3. Ensure that all Forms FD-500 that are submitted to the Asset Management Unit are complete, accurate and timely. Specifically, the FBI should ensure that the contents of the lost or stolen laptop computers accompany the Form FD-500.

4. Revise the Form FD-500 to include:

   (a) whether or not the loss was reported to the Inspection Division for investigation;

   (b) separate designation for "sensitive" and "classified" categories;

   (c) tracking of the classification level of NSI contained on a laptop;

   (d) whether sensitive information contained personally identifying

information; and

(e) whether the lost or stolen laptop computer was protected with encryption software.

5. Ensure that the Security Division performs a damage assessment of all laptops that are lost or stolen and maintains documentation on this information.

6. Ensure that weapon and laptop losses are appropriately entered into NCIC.

7. Assign to the Asset Management Unit monitoring responsibilities over weapon and laptop losses to ensure that all proper notifications are made.

II. INTERNAL CONTROLS

In our 2002 audit, we reported that the FBI failed to give sufficient priority to property management. Periodic inventories of accountable property were not conducted, departing employees did not always return all property that had been issued to them, and the destruction of outdated, damaged, or excessed laptop computers was not adequately documented. Additionally, while the FBI documented the disposal of laptop computers, it did not adequately document that all sensitive or classified information had been sanitized prior to their disposal. In our follow-up audit we noted improvements in the areas of conducting physical inventories and reconciling property records to the financial records. However, we identified continued weaknesses in several areas. Specifically, the FBI failed to adequately: (1) maintain records on how many of its laptop computers were authorized to process NSI; (2) improve its documentation of the disposal of excess laptop computers and hard drives to ensure that all sensitive or classified information had been sanitized prior to disposal; (3) report weapon and laptop losses to the DOJ; (4) submit incident reports of lost or stolen laptop computers to DOJCERT; and (5) improve the process to ensure that property is recovered from employees before they leave FBI service.

Physical Inventories

The DOJ Property Management Regulations requires all components to conduct an annual physical inventory of all non-expendable personal property. At the discretion of the component head, however, these inventories can be conducted every 2 years rather than annually.

The FBI's regulations require an annual inventory of all sensitive capitalized assets and sensitive property items, which include weapons and laptop computers. The FBI is also required to conduct a full inventory of all property and equipment every 2 years.

In our 2002 audit report, we concluded that the FBI failed to give sufficient attention to property management. The FBI chronically failed to complete the required biennial physical inventories of accountable property. Therefore, we recommended that the FBI conduct biennial inventories of accountable property and implement a policy requiring annual inventories of sensitive items, such as weapons and laptops.

The FBI concurred with our recommendations and notified all of its divisions that, effective with the 2003 biennial inventory, completion of biennial inventories of all accountable property and annual inventories of sensitive items, including weapons and laptop computers, was required. The policy also stated that the inventory of weapons would include issued weapons as well as weapons stored in the gun vault.

During our follow-up audit, we reviewed FBI-wide inventory reports for the years 2003 through 2005. We noted that the FBI had completed biennial inventories of all accountable property and annual inventories of sensitive items, including weapons and laptop computers. We believe that this completion of regular inventories improved the FBI's ability to account for and control its weapons and laptop computers.

Reconciling Property Records to the Financial System

In our 2002 audit report, 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. We recommended that the FBI implement a policy requiring that property records be reconciled with financial records to ensure the completeness of the FBI's property records.

In response to this recommendation, the FBI stated that the Asset Management Unit and Contract Unit would coordinate to ensure that the PMA was updated manually to include purchases of non-capitalized property. Further, FBI divisions were instructed to generate and review on-order reports on a monthly basis to ensure that newly purchased property was added to the PMA.[69] In addition, the Asset Management Unit generated delinquent on-order reports and distributed them to the appropriate APOs for follow-up.

In our follow-up review, we determined that the FBI's financial system was still not fully integrated with the PMA, although all divisions currently have the capability to generate an on-order report. In addition, we verified that FBI divisions have been instructed to generate the report on a monthly basis to review newly purchased property that should be placed in the PMA. We also noted that the Asset Management Unit generates delinquent on-order reports and distributes all copies to the APOs for follow-up. At the time of our follow-up review the FBI, in collaboration with the DOJ, was

[69] An on-order report reflects capitalized and non-capitalized property valued at $1,000 and above, and also sensitive property that should be entered into the PMA.

planning for future replacement of the Financial Management System and PMA systems with the implementation of the Unified Financial Management System (UFMS). The UFMS will replace financial systems DOJ-wide, integrating them with property management systems. The FBI expects that it will begin implementing the UFMS in December 2006. However, the process will not be completed until October 2009 and the FBI is not projected to begin processing transactions in the UFMS until Fiscal Year 2010.

During our follow-up review, we judgmentally selected 10 disbursements for the purchase of weapons since February 1, 2002, traced all the purchases to the PMA, and noted no discrepancies. The disbursements related to the purchase of 455 weapons.

We also judgmentally selected 10 disbursements for the purchase of laptops since February 1, 2002, traced all the purchases to the PMA, and again noted no discrepancies. The disbursements related to the purchase of 108 laptops.

As a result of our follow-up review, we determined that the FBI had implemented a sufficient policy requiring that property records be reconciled to the financial records to ensure the property records are complete.

Accuracy and Completeness of Property Records in the PMA

In our 2002 audit, we performed two tests to determine the accuracy and completeness of the PMA. We judgmentally selected weapons and laptop computers from the PMA and physically verified their existence. We also judgmentally selected items that were physically located at selected field and headquarters offices and traced them to the PMA. In our 2002 audit the FBI was able to provide all weapons and laptop computers for our physical verification.

During our follow-up audit, we performed the same two tests to determine the accuracy and completeness of the PMA. First, we selected a random sample of 497 weapons and 477 laptop computers from the PMA and physically verified their existence. We evaluated property records and property management activities at FBI headquarters and offices in New York, New York; Los Angeles, California; Washington, D.C.; Chicago, Illinois; and Miami, Florida.[70] We also tested the completeness of the property records by selecting a sample of 10 weapons and 10 laptop computers held at each

[70] The universe of weapons and laptop computers for each audited location and details of our sample, by property type, location, and type of test, appear in Appendix II.

of the field offices. We reviewed and traced them to the PMA and found no discrepancies.

To test the accuracy and completeness of the property records, we selected a sample of 974 items – 497 weapons and 477 laptop computers – recorded in the PMA and physically verified their existence. The FBI was able to provide all weapons and laptop computers for our physical verification, except for one weapon and two laptop computers assigned to FBI headquarters for which they provided confirmations of their existence. The following table summarizes our testing.

TOTAL SAMPLE ITEMS TESTED

	WEAPONS TESTED AND VERIFIED				LAPTOPS TESTED AND VERIFIED			
Location	**PMA**		**FLOOR**		**PMA**		**FLOOR**	
	Tested	**Verified**	**Tested**	**Verified**	**Tested**	**Verified**	**Tested**	**Verified**
FBI HQ	260	260	10	10	348	348	10	10
New York	69	69	10	10	42	42	10	10
Los Angeles	55	55	10	10	29	29	10	10
Washington, D.C.	44	44	10	10	24	24	10	10
Chicago	36	36	10	10	16	16	10	10
Miami	33	33	10	10	18	18	10	10
TOTALS	**497**	**497**	**60**	**60**	**477**	**477**	**60**	**60**

Source: OIG analysis of FBI PMA data

In addition to selecting a sample to verify the accuracy and completeness of the property management records, we analyzed the universe of 52,263 weapons and 26,166 laptop computer recorded in PMA as of November 2005 to ensure that data was entered properly for 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.[71] For weapons, we found 260 cost center names and 39 serial numbers were blank. For computers, we found that 864 cost codes, 971 cost center names, 92 serial numbers and 38 model numbers were blank. There were also 10,424 laptop computers that were not assigned to FBI personnel. However, during our audit the FBI took corrective action to assign laptops to its personnel, and as of May 2006 the FBI had only 124 unassigned laptop computers.[72]

[71] The PMA uses a variety of data fields to identify each item, including a barcode number assigned by the FBI, serial number, cost center code for the office where the item is located, description of the item, and other necessary information.

[72] See Appendix X for an analysis of the FBI's property records.

Reporting Requirements for Laptop Computers Containing NSI

In our 2002 audit, we reported that the FBI maintained records indicating which of its laptop computers were authorized to process classified information. Specifically, the FBI had a total of 10,003 laptop computers with the following security levels: 5 Top Secret; 8,000 Secret; 1,711 unclassified; and 287 miscellaneous (damaged, no hard drive, unusable). However, during our follow-up audit, FBI officials told us that they no longer maintained this type of information.

The DOJ's Office of the Chief Information Officer (DOJ CIO) requires the FBI to report the number of laptop computers it has authorized for processing classified information. To ensure that the FBI complied with the requirement, during our follow-up audit we requested this information from the FBI and the DOJ CIO, but neither could provide it. FBI officials informed us that they did not track such information and the DOJ CIO confirmed that the FBI had not provided it to them. However, the DOJ CIO requested that the FBI provide a report containing the information by June 4, 2006.

Prior to DOJ's CIO requests, the FBI deployed the PED Application to register all FBI electronic devices, including laptop computers. The PED Application draws baseline information from the FBI's PMA and requires users to register their assigned devices and to indicate the security classification of each device. FBI officials told us that they are in the process of completing the registration for the FBI's approximately 23,000 laptops. As of September 14, 2006, the FBI had provided information containing classification levels for 1,925 of its approximately 25,000 laptop computers.

Although the FBI deployed the PED Application to begin to track security classification levels in June 2006, the FBI did not maintain records indicating the classification of its laptop computers prior to the implementation of the PED.

Reporting Losses to DOJ

DOJ Semiannual Theft Reports

DOJ regulations require all components to submit to DOJ semiannual reports summarizing thefts of government property that occurred within the preceding 6 months from January 1 and July 1. In our 2002 audit, we found that four of the five Semiannual Reports submitted by the FBI to the DOJ

were submitted late, ranging from 6 to 106 days.[73] In addition, the semiannual reports were inaccurate with respect to the number of weapon and laptop losses. We recommended that the FBI submit complete, accurate, and timely semiannual reports to the DOJ.

Our follow-up review found that the FBI has not corrected these deficiencies. The FBI did not submit a semiannual report for the period between January 1, 2002, and June 30, 2002. The overall period covered by the reports that we reviewed were submitted from July 1, 2002, through December 31, 2005. We reviewed the seven semiannual reports submitted by the FBI during the audit period and found all the reports to contain incomplete and inaccurate information. Although the reports listed the barcode numbers, descriptions, dollar values, and location of items, some reports did not contain the date of the incident. Further, when the reports asked whether corrective measures were taken to prevent repetition and the status of the actions taken, the answer was given as "unknown."

During the period covered in our follow-up review, FBI records documented the loss or theft of 160 weapons and 160 laptop computers. However, in the semiannual reports the FBI reported to the DOJ only 106 lost and stolen weapons and 97 lost and stolen laptop computers, as shown in the table below.

[73] DOJ Semiannual Reports should contain the following information: description, indicating if government or personal property; serial number, if any; dollar value; date and location of incident; results of any investigation conducted by the appropriate agency; and any corrective measures taken to prevent repetition. Loss or theft of ADP equipment shall also include the following: a copy of the Federal Protective Service or other investigative report; and a statement from the owner or user of the ADP equipment categorizing the information as NSI, sensitive information or non-sensitive information.

ACCURACY OF FBI'S SEMIANNUAL REPORTS TO THE DOJ

Semi-Annual Period Ended	Weapon Losses		Laptop Computer Losses		Total	
	Reported to DOJ	FBI Property Records	Reported to DOJ	FBI Property Records	Reported to DOJ	FBI Property Records
06/30/02	NA	40	NA	11	NA	51
12/31/02	22	20	21	21	43	41
06/30/03	17	17	14	12	31	29
12/31/03	23	34	22	41	45	75
06/30/04	12	12	21	42	33	54
12/31/04	4	4	4	6	8	10
06/30/05	20	27	10	24	30	51
12/31/05[74]	8	6	5	3	13	9
TOTALS	**106**	**160**	**97**	**160**	**203**	**320**

Source: OIG analysis of FBI data

Further, only 4 of the 10 laptop computers that were identified as having sensitive or classified information were reported to the DOJ. The remaining six were not reported. Only 30 of the 51 laptop computers that were unknown as to whether they contained sensitive or classified information were reported to the DOJ. In our judgment, the FBI has not adequately improved its procedures relating to the timely and accurate reporting of thefts of government property to the Justice Management Division, Facilities and Administrative Services Staff (FASS) DOJ Security Officer.

DOJCERT

DOJ regulations require all components to submit immediate reports summarizing incidents involving the loss of both classified and unclassified systems, to the Department of Justice Computer Emergency Response Team (DOJCERT). The DOJCERT assists in handling computer security incidents throughout DOJ.[75]

We contacted DOJCERT officials to determine if the FBI submitted the required incident reports for the 160 laptop computers that were identified as lost or stolen during our review period. We determined that of the 160

[74] The DOJ Semiannual Report ending December 31, 2005, contained information relating to lost or stolen weapons and laptop computers that occurred during the audit period ending September 30, 2005. Our analysis did not include losses that occurred after September 30, 2005.

[75] According to the DOJCERT, computer security incidents are any unexpected, unplanned event that could have a negative impact on IT resources. Computer security incidents can include the loss of both classified and unclassified systems, unauthorized removal of computer equipment, and exploited weaknesses in a computer system that allows unauthorized access to password files.

laptops that FBI reported as lost or stolen during the 44-month review period, it had only submitted 1 incident report to the DOJCERT. This incident report contained information regarding a laptop computer that contained sensitive information reported stolen by the FBI's Criminal Justice Information Services (CJIS) Division on June 24, 2005. The FBI did not report any of the other lost or stolen laptop computers to the DOJCERT, including the other 9 that the FBI believed contained sensitive or classified information.

We asked the FBI's Enterprise Security Operations Center (ESOC), the unit responsible for submitting incident reports summarizing computer losses, why only one incident was reported to the DOJCERT. In response, the ESOC officials stated that prior to an OMB memorandum, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* dated July 12, 2006, the FBI was only responsible for submitting incidents to the DOJCERT that pertained to the loss of Personally Identifiable Information.[76] However, as stated previously, as a result of our review we identified a stolen laptop containing the names, addresses and phone numbers of FBI personnel that was not reported to the DOJCERT. Further DOJCERT officials told us that the reporting of incidents involving the loss of both classified and unclassified systems to the DOJCERT has been a requirement since the inception of the United States Computer Emergency Readiness Team (US-CERT) in 2003.[77]

Disposal of Weapons and Laptop Computers

In our 2002 audit report, we found that the documentation for laptop disposals did not establish whether hard drives were properly destroyed and disposed of and were free of classified information. We recommended that the FBI improve the documentation showing that outdated, damaged, or excess laptop computers and hard drives were properly discarded.

[76] Personally Identifiable Information is any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to an individual.

[77] The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

In response to this recommendation, the FBI said it would implement an automated system for tracking information technology throughout its life cycle, including its disposal. Further, the FBI Security Division issued guidance in November 2003 governing the improved documentation of the destruction of excess laptops and hard drives. The guidance specifically addressed the clearing, sanitization and destruction of all media types, including computer hard drives.

However, the guidance does not specifically include the requirement for documenting that laptops and other media are properly discarded.

The MAOP requires that all computers that have processed sensitive or classified information be "sanitized and declassified" and sent to FBI headquarters for disposal. Field offices are required to initiate the disposal of excess laptop computers by entering a "Declaration of Excess" and an "Excess Property Detail Report" into the PMA as well as by submitting to the Asset Management Unit a Form FD-519 (Requirements and Certification for Cannibalization and Destruction of Equipment).

During our follow-up audit at FBI headquarters, we obtained Forms FD-519 that included laptop computers, which were disposed of between February 1, 2002, and September 30, 2005. We selected a judgmental sample of ten laptop computers from the Forms FD-519 and traced them to the PMA, confirming that the PMA accurately showed the excess laptops as disposed.

At the five field offices we visited, the available documentation pertaining to hard drives from excessed laptops did not indicate that the field offices removed hard drives and sent them to FBI headquarters for disposal. The available documentation that we examined also did not include evidence of whether any classified information had been sanitized. Further, we found evidence at the Los Angeles Field Office and the New York Field Office 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 were told that all hard drives from Los Angeles and New York were degaussed and destroyed at the field office instead of being forwarded to FBI headquarters.[78] The New York Field Office received degaussing equipment in June 2006; however, it had not forwarded hard drives to FBI Headquarters for more than 2 years. Records at FBI headquarters also did not sufficiently document that hard drives from field

[78] Degaussing is the process of erasing data that is stored in magnetic media, such as hard drives, floppy disks and magnetic tape, thereby rendering previous data unrecoverable.

offices were received and properly destroyed. Specifically, the records did not include names of employees, the reason for destruction, and the location and method of destruction, as required. Further, the FBI policy states that the destruction of Top Secret and Sensitive Compartmented Information (SCI) must be witnessed and recorded by two employees with security clearances commensurate with the classification of the material being destroyed. We cannot be certain that the FBI followed the policy since we could not determine if any of the hard drives that were destroyed contained Top Secret or SCI information.

In sum, despite our prior recommendation, the FBI did not document that specific computers had been "sanitized and declassified" before being disposed. Officials at each of those locations told us they believed that excess laptop computers and hard drives had been properly discarded. However, they could not provide evidence that proper procedures were followed. We again recommend that the FBI document the completion of all required steps for disposing of excess laptop computers and hard drives that previously processed sensitive or classified information.

Exit Procedures for Departing Employees

In our 2002 audit report, we found indications that the FBI was not recovering all issued weapons and laptops from employees before their departure. We recommended that the FBI strengthen procedures to ensure departing employees return all property issued to them or reimburse the government. In response to the recommendation, the FBI revised its policy and distributed an electronic communication to all employees who were leaving, notifying them that they could be held accountable for lost or stolen FBI property.

The process for departing FBI employees 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 and recover all issued property listed on that document. In addition, the supervisor should complete a Report of Exit and Separation (Form FD-193) and a Receipt for Government Property (Form FD-281). The Form FD-281 is used for both receiving and returning government property. The Form FD-193 documents a variety of actions that must be completed upon an employee's departure.

During our follow-up review, we judgmentally selected the files of 50 former employees and the Forms FD-281 and FD-193 for both weapons and laptops issued to each of the 50 employees. We asked for these documents at both the FBI Records Management Division and at each of the field offices that we reviewed. However, the FBI could provide only 19 of the required

50 Forms FD-281 for weapons and laptop computers, and only 32 of the 50 Forms FD-193.

The following table shows the number of Forms FD-281 and the Forms FD-193 reviewed for the five field offices.

TOTAL FORMS FD-281 AND FD-193 REVIEWED FEBRUARY 1, 2002, THROUGH SEPTEMBER 30, 2005

	New York	Los Angeles	Washington D.C.	Chicago	Miami	TOTALS
FD-281 Weapons	3	10	2	0	2	**17**
FD-281 Laptop Computers	0	2	0	0	0	**2**
FD-193	10	6	5	6	5	**32**

Source: OIG analysis of FBI data

Based on our review of the 160 weapon losses, we concluded that four of the lost or stolen weapons were the result of an agent leaving the FBI and not returning a weapon. In our judgment, the FBI has not sufficiently strengthened its exit processing for departing employees to obtain all weapons.

The FBI also revised its policy to require that all laptop computers issued to an individual be documented on a Form FD-281. The forms should be signed by the individual with custody of the property and maintained at the division office. We did not find any cases that resulted in an agent leaving the FBI and not returning a laptop.

In sum, although the FBI revised its policy to strengthen procedures to ensure that departing employees return all property that had been issued to them or reimburse the government for the cost of the property, we noted that the policy is not being followed consistently.

Conclusion

In response to our August 2002 audit, the FBI has taken steps to address weaknesses in physical inventories and reconciling weapons and laptop computers to the financial system. However, we identified continuing weaknesses in several areas. Specifically, the FBI failed to adequately: (1) maintain records on how many of its laptop computers were authorized to process NSI; (2) improve its documentation of the disposal of excess laptop computers and hard drives to ensure that all sensitive or classified information had been sanitized prior to disposal; (3) report weapon and

laptop losses to the DOJ; and (4) ensure that property is recovered from employees before they leave FBI service. Therefore, we make several recommendations for the FBI to improve its management of weapons and laptop computers.

Recommendations

We recommend that the FBI:

8. Maintain and submit complete, accurate, and timely reports to the DOJ CIO containing all appropriate FBI laptops authorized to process classified information.

9. Improve the documentation supporting the destruction of excess laptop computers and hard drives.

10. Revise its guidance regarding when field offices can degauss their own hard drives.

11. Submit complete, accurate, and timely Semiannual Reports to the DOJ Security Officer JMD, FASS.

12. Submit complete, accurate, and timely incident reports summarizing the loss of appropriate FBI laptop computers to the DOJCERT, as required.

13. Strengthen the exit processing for departing employees to ensure that all weapons, laptops, and other issued property is returned to the FBI.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

The audit of the FBI's control over weapons and laptop computers was conducted in accordance with *Government Auditing Standards*. As required by these standards, we tested selected transactions and records to obtain reasonable assurance about the FBI's compliance with laws and regulations that, if not complied with, we believe could have a material effect on operations. Compliance with laws and regulations applicable to the FBI's control over weapons and laptops is the responsibility of its management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific requirements for which we conducted tests are contained in the OMB Circular No. A-123, *Management's Responsibility for Internal Control* and the Justice Property Management Regulations (JPMR).

Our audit identified several areas where the FBI was not in compliance with the laws and regulations referred to above. Specifically, the FBI did not always report its lost and stolen weapons and laptops to DOJ as required. In addition, the FBI did not always report incidents pertaining to lost or stolen laptop computers to DOJCERT as required. With respect to transactions that were not tested, nothing came to our attention that caused us to believe that FBI management was not in compliance with the laws and regulations cited above.

STATEMENT ON MANAGEMENT CONTROLS

In planning and performing our audit of the FBI's Controls over Weapons and Laptop Computers, we considered the FBI's management controls for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the management control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the management control structure that, in our judgment, could adversely affect the FBI's ability to manage its control over weapons and laptops. During our audit, we identified the following management control concerns.

- The FBI does not maintain records of laptops with NSI classification levels as required by the DOJ CIO.

- The FBI failed to improve its documentation of the disposal of excess laptop computers and hard drives to ensure that all sensitive or classified information had been sanitized prior to disposal.

- The FBI failed to improve the process to ensure that property is recovered from employees before they leave the FBI.

Because we are not expressing an opinion on the FBI's management control structure as a whole, this statement is intended solely for the information and use of the FBI in managing its control over weapons and laptops. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

We completed a follow-up audit of the FBI's control over weapons and laptop computers. The purpose of the follow-up audit was to assess whether adequate corrective action had been taken on findings and recommendations in the August 2002 audit report. Those recommendations stated that the FBI should: (1) revise its policy for protecting equipment from loss and for disciplining employees when they do not follow FBI policy; (2) establish deadlines for reporting, documenting, and investigating losses, (3) ensure that the FBI conducts periodic inventories of weapons and laptop computers; (4) reconcile the property records to the financial records; (5) ensure that departing employees return all property that was entrusted to them; and (6) improve documentation showing that excess property had been properly disposed. The FBI agreed with these recommendations and outlined a plan for taking corrective action.

We performed the follow-up audit in accordance with the *Government Auditing Standards* and included such tests of the records and procedures that we considered necessary. Our testing covered the period between February 1, 2002, and September 30, 2005.

We obtained an understanding of the control environment for weapons and laptop computers from the Property Procurement and Management Section of the Finance Division at FBI headquarters. We performed on-site audit work between October 2005 and June 2006 at FBI headquarters (including the Training Academy at Quantico, Virginia) and at field offices in New York, New York; Miami, Florida; Los Angeles, California; Chicago, Illinois; and Washington, D.C.

To examine the FBI's efforts to identify lost and stolen weapons and laptop computers, we obtained a list of all such losses that occurred since February 1, 2002, and reviewed the available files and the circumstances surrounding those losses. We also obtained DOJ Semi-annual Reports of lost or stolen property that were submitted to the DOJ Security Officer. For lost or stolen weapons, we queried NCIC to determine if those losses had been reported and if weapons had been subsequently recovered. We also queried the ATF National Tracing Center database to determine if any of those weapons had been recovered through subsequent law enforcement activities.

For laptop computers, our objective was to determine if the loss resulted in compromised classified or sensitive information. We could not

independently verify the sensitivity of the information due to the loss of the machines. Therefore, we relied on assertions from the Reports of Lost or Stolen Property (Form FD-500) submitted for each lost or stolen laptop to ascertain whether classified or sensitive information was comprised.

In addition to the testing detailed above, we: (1) reviewed applicable laws, policies, regulations, manuals, and memoranda; (2) interviewed appropriate personnel; (3) tested internal controls; (4) reviewed property and accounting records (with an emphasis on activity since February 1, 2002); and (5) physically inspected property. We tested internal controls pertaining to weapons and laptop computers in the following areas:

- purchasing and recording in the official property database, the PMA;
- receipt and assignment, including weapons and laptop computers not assigned to specific individuals (pooled property), specialized equipment, and the return of items from separated employees;
- physical inventories, including separation of duties; and
- disposals, including property record deletions.

We tested these controls through a sample from the 52,263 weapons and 26,166 laptop computers reported in the PMA as of November 2005. In total, we reviewed 974 items, including 497 weapons and 477 laptop computers. Details about the universe from which these samples were taken and about the samples themselves may be found in Appendix II. Our tests also included:

- samples of weapons and laptop computers purchased between February 1, 2002, and September 30, 2005, as recorded in purchase documents, to ensure that the items were recorded in the PMA;
- samples of pooled property to ensure that the property was accounted for and the records reflected the correct status;
- samples of weapons and laptop computers found during an on-site inventory at each audited FBI location to ensure that the item was accurately reflected in the PMA; and
- samples of weapons and laptop computers assigned to FBI personnel to ensure the items were accounted for and the property records were complete (staff testing).

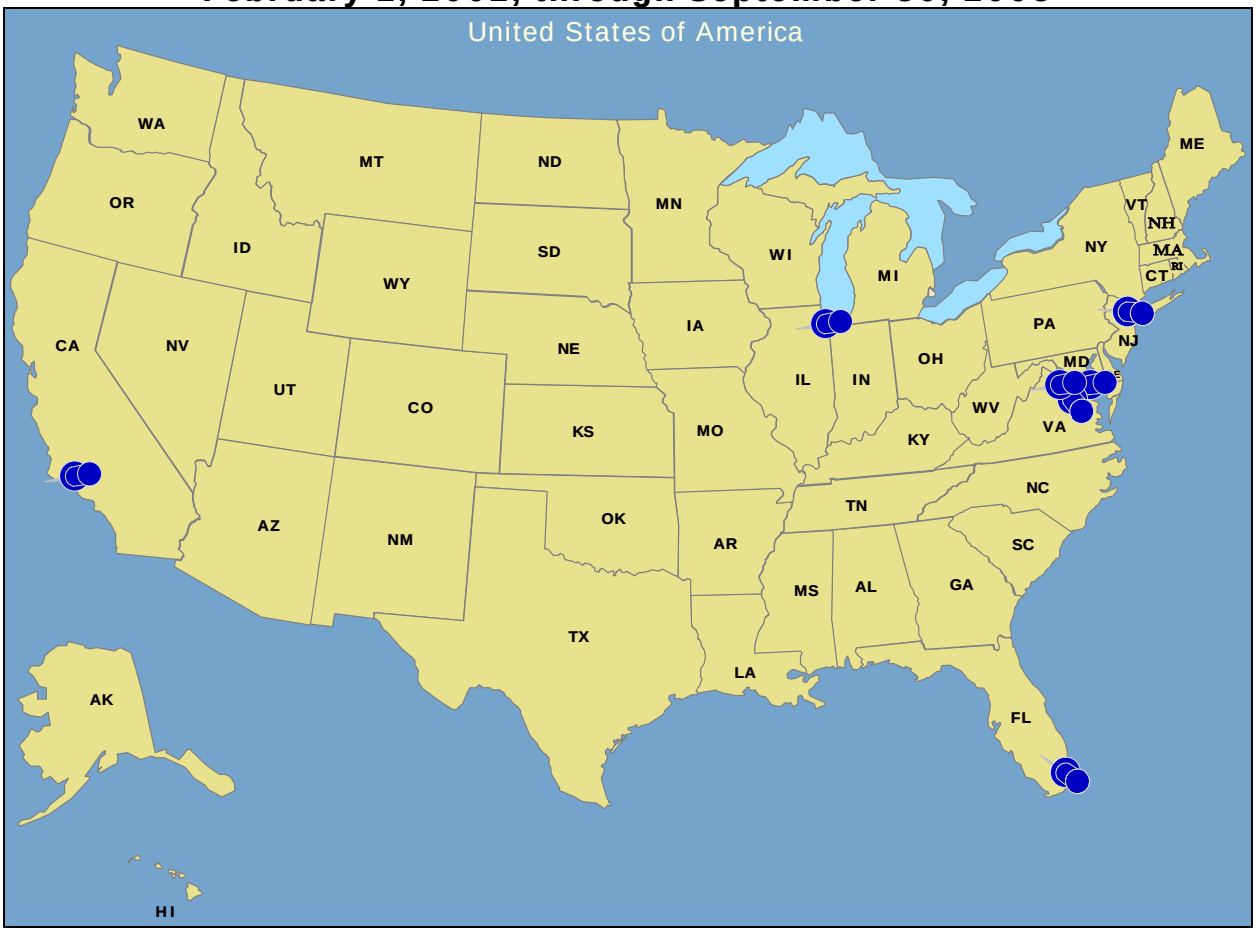
The samples described above are delineated by test, property type, and location, in the table in Appendix II. We also reviewed the documentation between February 1, 2002, and September 30, 2005, related to 50 former FBI personnel, to determine if all weapons and laptop computers were returned. Moreover, we reviewed disposal actions initiated between February 1, 2002, and September 30, 2005, to ensure these actions were adequately supported.

APPENDIX II

SAMPLING DESIGN

The FBI database we tested contained 52,263 weapons and 26,166 laptops assigned to all FBI offices and officials located around the country and abroad. Analysis of the distribution of weapons and laptops revealed that more than half of the items in the universe were assigned to seven offices. Specifically, 52 percent of all weapons and 54 percent of all laptops were assigned to: (1) FBI headquarters, (2) the FBI Training Academy at Quantico, Virginia, (3) the Chicago Field Office, (4) the Los Angeles Field Office, (5) the Miami Field Office, (6) the New York City Field Office, and (7) the Washington, D.C. Field Office.

Seven Offices Reviewed
February 1, 2002, through September 30, 2005



Source: OIG analysis of FBI data

To provide effective coverage and efficient testing of the items, a stratified random sample design was selected, as shown in the table below. A total sample of 497 weapons and 477 laptops were tested.

Sample of Weapons and Laptop Computers Tested

Location	Weapons		Laptops	
	Number Tested	Percent Tested	Number Tested	Percent Tested
Quantico, VA	212	1.17%	187	3.24%
FBI Headquarters	48	2.92%	161	3.16%
Chicago	36	3.17%	16	4.03%
Los Angeles	55	3.18%	29	4.02%
Miami	33	3.20%	18	4.00%
New York	69	3.17%	42	4.03%
Washington, D.C.	44	3.18%	24	3.99%
Total	**497**		**477**	

Source: Property Management Application (PMA) System

APPENDIX III

CIRCUMSTANCES OF WEAPON LOSSES

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
1 [80]	08/10/01	Los Angeles	Special Agent's rental vehicle was burglarized. Weapon and other items in the trunk were stolen.
2	12/18/01	Washington	Special Agent's FBI vehicle was stolen. The weapon was inside the vehicle.
3	01/11/02	Los Angeles	Unexplained Loss.
4	01/11/02	Los Angeles	Special Agent retired. No record of having returned his weapon.
5	01/25/02	New York City	Weapon stolen from Special Agent's residence. **Issuance of letter of censure.**
6	01/25/02	New York City	Weapon stolen from Special Agent's FBI vehicle.
7	01/25/02	New York City	Weapon stolen from Special Agent's FBI vehicle.
8	01/31/02	Pittsburg	The weapon was reported as stolen from the Special Agent's desk.
9	02/11/02	New York	Special Agent mugged and weapon was stolen.
10	02/20/02	Milwaukee	Special Agent retired from the FBI on 11/30/93. Special Agent stated that he surrendered his bureau weapon to an individual in the Milwaukee office.
11	02/26/02	Miami	Special Agent who resigned from the FBI claimed that he had turned in the weapon to a Principal Firearms Instructor at an unknown time. However, records reflected that the missing pistol was still listed as assigned to the Special Agent.
12	02/26/02	Miami	Before the Special Agent retired, his home was burglarized and his Bureau issued weapon was stolen.
13	02/28/02	Albany	Unable to find weapon during the inventory.
14	02/28/02	Albany	Unable to find weapon during the inventory.
15	02/28/02	Albany	Unable to find weapon during the inventory.
16	02/28/02	Albany	Unable to find weapon during the inventory.
17	02/28/02	Albany	Unable to find weapon during the inventory.

[79] In the Description of Loss column, we added in bold the result of OPR's adjudication of the loss.

[80] While weapon losses 1 through 8 occurred prior to our audit period beginning February 1, 2002; we included them in our audit because they were reported during the period of our review.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
18	02/28/02	Birmingham	Unable to find weapon during the inventory.
19	02/28/02	Los Angeles	Weapon Stolen from Special Agent's FBI vehicle.
20	02/28/02	Dallas	Unexplained loss.
21	03/05/02	Dallas	Weapon Stolen from Special Agent's FBI vehicle. **Issuance of letter of censure.**
22	03/12/02	Washington	Unknown
23	03/12/02	Washington	Unknown
24	03/12/02	Washington	Unknown
25	03/12/02	Unknown	No explanation.
26	03/12/02	Washington	Unknown
27	03/13/02	Albany	Unable to find weapon during the inventory.
28	03/13/02	Albuquerque	Weapon Stolen from Special Agent's residence.
29	03/15/02	New York	While in a restaurant, Special Agent's briefcase was stolen containing the weapon.
30	03/20/02	Richmond	Unable to find weapon during the inventory.
31	04/03/02	Boston	Special Agent stated that he never took possession of the weapon having only signed it out to take advantage of the buyback program that was being proposed at the time. The missing weapon is considered lost.
32	04/03/02	Salt Lake City	Weapon was not returned by terminated employee.
33	04/03/02	Tampa	Weapon stolen from rental car.
34	04/03/02	Oklahoma City	The retired Special Agent stated that during his undercover assignment, his desk was cleaned out by other agents. The Special Agent also stated that the weapon was returned to the WMF at Quantico.
35	04/03/02	New York City	Special Agent retired. No record of having returned his firearm.
36	04/04/02	Phoenix	Special Agent's car was stolen. When the vehicle was recovered, the weapon was missing.
37	04/6/02	Unknown	Weapon stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
38	04/25/02	Unknown	Weapon stolen from Special Agent's FBI vehicle.
39	05/09/02	New York City	Weapon stolen from a locked drawer located in secure Bureau space.
40	05/13/02	Washington	Special Agent's fanny pack containing gun was stolen from a storage room.**3-day suspension.**
41	05/14/02	Oklahoma City	The property has not been located during the Oklahoma City Division's physical inventory. A thorough review of OC's Administrative files failed to locate any documentation concerning the property.
42	05/23/02	Washington	Weapon stolen from Special Agent's POV. **3-day suspension.**
43	06/20/02	Knoxville	Special Agent stated he returned the weapon into the gun vault at FBI Headquarters in 2000. However, there is no documentation as to the weapon being returned. **3-day suspension without pay.**
44	06/20/02	Unknown	Special Agent was mugged and weapon stolen.
45	07/10/02	Atlanta	Stolen from FBI vehicle. **3-day suspension without pay.**
46	07/22/02	Oklahoma City	Retired Special Agent turned in his revolver in approximately 1986, when he was issued a semi-automatic pistol. The property has not been located during an Oklahoma City Division's physical inventory.
47	08/12/02	Oklahoma City	Weapon was stolen during a burglary of his residence.
48	08/19/02	Sacramento	Weapon was stolen from hotel burglary.
49	08/19/02	Minneapolis	Weapon was stolen from Special Agent's FBI vehicle**.** **5-day suspension without pay.**
50	08/21/02	Salt Lake City	No explanation
51	08/21/02	Salt Lake City	Weapon was stolen from hotel burglary. **Letter of censure was issued to the Special Agent.**
52	08/26/02	Jackson	Special Agent advised the FBI during an interview that he returned his weapon to the gun vault on 5/7/91. Weapon could not be found during the inventory.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
53	08/27/02	Baltimore	Weapons stolen from Special Agent's FBI vehicle. **Letter of censure**
54	09/09/02	Miami	No explanation
55	09/16/02	Miami	Weapons stolen from Special Agent's FBI vehicle. **5-day suspension without pay.**
56	09/23/02	Charlotte	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
57	10/11/02	New Orleans	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
58	10/15/02	Washington	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension.**
59	10/17/02	Los Angeles	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
60	10/31/02	San Francisco	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension.**
61	11/22/02	New York City	Weapons stolen from Special Agent's FBI vehicle.
62	12/02/02	Houston	Weapons stolen from Special Agent's FBI vehicle.
63	12/11/02	Albuquerque	Fanny pack containing weapon was left and lost in shopping cart at a grocery store. **3-day suspension without pay.**
64	01/06/03	Albuquerque	Weapons stolen from Special Agent's residence.
65	01/08/03	San Francisco	Weapon was stolen from FBI vehicle parked at the Special Agent's residence. **3-day suspension without pay.**
66	01/09/03	Cleveland	Weapons stolen from Special Agent's FBI vehicle.
67	01/13/03	Houston	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
68	02/03/03	Albuquerque	Weapons stolen from Special Agent's FBI vehicle.
69	02/03/03	Albuquerque	Weapons stolen from Special Agent's FBI vehicle.
70	02/10/03	Michigan	Weapons stolen from Special Agent's FBI vehicle.
71	02/27/03	Honolulu	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
72	03/03/03	Chicago	Weapons stolen from agent's residence.
73	03/13/03	Miami	Weapons stolen from Special Agent's FBI vehicle.
74	03/25/03	Boston	Weapon could not be located during the inventory.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
75	03/25/03	Boston	Weapon could not be located during the inventory.
76	03/25/03	Boston	Weapon could not be located during the inventory.
77	03/26/03	Miami	Weapons stolen from Special Agent's FBI vehicle.
78	05/14/03	Los Angeles	Weapons stolen from Special Agent's FBI vehicle.
79	05/16/03	Unknown	Weapon could not be located during the inventory.
80	06/05/03	Unknown	Weapon could not be located during the inventory.
81	06/06/03	Houston	Weapons stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
82	06/20/03	Unknown	No explanation.
83	06/26/03	New York	Special Agent's residence was burglarized and the weapon stolen.**3-day suspension without pay.**
84	06/30/03	Phoenix	Weapon stolen from Special Agent's FBI vehicle.
85	07/08/03	Boston	Weapon stolen from Special Agent's FBI vehicle. **Issuance of letter of censure.**
86	07/08/03	Richmond	Weapon stolen from Special Agent's FBI vehicle. **3-day suspension without pay.**
87	07/10/03	Omaha	Paint gun may have been stolen from a SWAT vehicle parked inside Special Agent's garage.
88	07/10/03	Omaha	Paint gun may have been stolen from a SWAT vehicle parked inside Special Agent's garage.
89	07/11/03	Detroit	Weapon could not be located during a physical inventory.
90	07/11/03	Mobile Vault	No explanation.
91	07/11/03	Mobile Vault	No explanation.
92	07/11/03	Mobile Vault	No explanation.
93	07/11/03	Mobile Vault	No explanation.
94	07/11/03	Mobile Vault	No explanation.
95	07/11/03	Mobile Vault	No explanation.
96	07/11/03	Mobile Vault	No explanation.
97	07/11/03	Mobile Vault	No explanation.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
98	07/14/03	Salt Lake	Weapon could not be located during a physical inventory.
99	07/15/03	Tampa	POV was stolen while the weapon was inside. The vehicle was recovered; however, the weapon was not in the vehicle.**3-day suspension without pay.**
100	07/16/03	Chicago	No explanation.
101	07/16/03	Boston	Weapon could not be located during the inventory.
102	07/16/03	Cleveland	Weapon could not be located during the inventory. Case was closed without an OPR inquiry.
103	07/21/03	Richmond	Weapon stolen from a locked vehicle owned by a Bedford County Sheriff's Office Investigator.
104	07/25/03	Sacramento	Special Agent's weapon was stolen while traveling on official business in San Francisco. No other details available.**3-day suspension without pay.**
105	08/13/03	New York City	Weapon stolen from burglarized residence.
106	08/26/03	Denver	Weapon stolen from FBI vehicle. **5-day suspension without pay.**
107	09/26/03	Philadelphia	Special Agent misplaced his personally-owned gunny sack containing his duty weapon. **3-day suspension.**
108	09/30/03	Philadelphia	Weapon stolen from FBI vehicle. **3-day suspension without pay.**
109	11/26/03	Tampa	Weapon stolen from FBI vehicle. **3-day suspension.**
110	12/30/03	Phoenix	Weapon stolen from FBI vehicle. **3-day day suspension without pay.**
111	01/15/04	Los Angeles	Weapon stolen from FBI vehicle. **5-day suspension without pay.**
112	03/03/04	Washington	Weapon stolen from FBI vehicle.
113	03/30/04	Columbia	Weapon stolen from rental car. **3-day suspension without pay.**
114	04/08/04	San Francisco	Weapon stolen from FBI vehicle.
115	04/08/04	San Francisco	Stolen from FBI vehicle.
116	04/16/04	San Antonio	Weapon stolen from office desk. **7-day suspension.**
117	04/26/04	Salt Lake	Weapon stolen from FBI vehicle.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
118	05/20/04	Indianapolis	Weapon stolen from FBI vehicle. Vehicle was locked and trunk chained.
119	06/24/04	New York	Rented vehicle was burglarized and weapon was stolen.
120	07/16/04	San Antonio	Special Agent was unable to produce weapon when terminated as an employee. **Agent was terminated for cause unrelated to loss of firearm.**
121	09/10/04	Dallas	No explanation.
122	10/04/04	San Juan	Weapon stolen from Special Agent's POV. **3-day suspension. FBI reported weapon found.[81]**
123	10/26/04	Los Angeles	Fanny pack containing weapon was stolen at a restaurant **5-day suspension without pay.**
124	11/04/04	Seattle	Special Agent's vehicle stolen from a parking lot with the weapon in the trunk. The vehicle was later recovered but had been completely destroyed by fire.
125	11/19/04	San Juan	Special Agent did not know whether weapon was stolen from FBI vehicle or restaurant **5-day suspension without pay.**
126	01/04/05	Dallas	Weapon stolen from Special Agent's FBI vehicle
127	01/05/05	New York	No explanation.
128	01/05/05	El Paso	Purse containing weapon was stolen from a Restaurant. **3-day suspension without pay.**
129	01/19/05	San Juan	Weapon stolen from Special Agent's FBI vehicle. **7-day suspension.**
130	01/19/05	San Juan	Weapon stolen from Special Agent's FBI vehicle.
131	01/24/05	Washington, DC	Weapon stolen from Special Agent's FBI vehicle.
132	03/01/05	San Antonio	No explanation.
133	03/03/05	New York	Weapon stolen from residence.

[81] After completion of our fieldwork, the FBI reported to us that seven weapons had been recovered.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
134	03/15/05	Philadelphia	Weapon stolen from residence. **7-day suspension.**
135	04/01/05	San Diego	Weapon stolen from POV. The weapon was a fanny bag which was secured in the trunk of the vehicle. **No disciplinary action. Agent retired on 4/3/2002. Loss occurred on 1/26/2002.**
136	04/01/05	New Orleans	Weapon stolen from Special Agent's FBI vehicle **FBI reported weapon found.**
137	04/28/05	Miami	Weapon could not be located by the NFPU while conducting the FY 2005 physical inventory.
138	05/05/05	Little Rock	No explanation.
139	05/06/05	Washington Field Office	Weapon could not be located during the inventory. **FBI reported weapon found.**
140	05/10/05	Jacksonville	Weapon was unaccounted for during a property inventory.
141	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
142	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
143	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
144	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
145	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
146	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
147	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
148	05/10/05	Atlanta	One of eight weapons stolen from the Atlanta Division SWAT van during the Super Bowl, held in Jacksonville, Florida on February 6, 2005.
149	05/25/05	Salt Lake	Special Agent did not return the issued weapon to NFPU following his retirement on April 30, 2002.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS[79]
150	06/07/05	Dallas	Purse containing weapon was stolen from a Sports Bar. **FBI reported weapon found. 7-day suspension without pay.**
151	06/17/05	Seattle	Special Agent stopped at a coffee shop for a restroom break and inadvertently left the store leaving his gun behind in a fanny pack.
152	07/01/05	Washington, DC	Weapon was stolen from POV glove compartment. **5-day suspension without pay.**
153	08/01/05	Richmond	Weapon stolen from Special Agent's FBI vehicle.
154	08/05/05	El Paso	Weapon stolen from Special Agent's FBI vehicle. **FBI reported weapon found.**
155	08/09/05	Omaha	Special Agent left duty sidearm in gas station restroom and upon returning the weapon was missing. **FBI reported weapon found.**
156	08/25/05	Milwaukee	Special Agent was found deceased in his residence. His weapon could not be found. **FBI reported weapon found.**
157	NA	FBI did not provide FD-500	No explanation.
158	NA	FBI did not provide FD-500	No explanation
159	NA	FBI did not provide FD-500	No Explanation
160	NA	FBI did not provide FD-500	No Explanation

APPENDIX IV

CIRCUMSTANCES OF LAPTOP LOSSES

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
1[82]	04/19/01	Washington	Laptop lost in transit from Rwanda to Washington DC	Special Agent not certain if classified information was contained on the hard drive.
2	08/17/01	San Antonio	Stolen from secured Bucar at agent's residence	CND[83]
3	10/25/01	Baltimore Special Ops Group	Office space was burglarized	CND
4	11/12/01	Salt Lake City	Burglarized at Special Agent's residence-**3-day suspension**	Laptop's hard drive had recently been wiped clean with no national security or law enforcement sensitive information.
5	12/06/01	FBI HQ	Unable to locate during physical inventory.	CND
6	01/25/02	New York	Bucar car was burglarized.	CND
7	02/27/02	Los Angeles	Bucar car was burglarized	CND
8	02/28/02	San Juan	Unable to locate during physical inventory.	CND
9	03/12/02	FBI HQ	Unable to locate during physical inventory.	CND
10	03/27/02	FBI HQ	Unknown	CND
11	04/11/02	FBI Laboratory	Lost when laptop was shipped for repair.	CND
12	05/02/02	Philadelphia	Bucar was burglarized.	CND
13	05/06/02	Salt Lake City	Luggage was left with hotel prior to check in. When Special Agent returned to retrieve luggage, the laptop was missing.	CND
14	05/16/02	Miami	Special Agent's residence was burglarized.	Laptop did not contain any files and was protected with Safeguard Easy for Windows 2000.
15	05/16/02	Kansas City	Bucar was burglarized.	CND

[82] While laptop losses 1 through 6 occurred prior to our audit period beginning February 1, 2002; we included them in our audit because they were reported during the period of our review.

[83] Cannot Determine.

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
16	06/24/02	Los Angeles	Special Agent's residence was burglarized.	Laptop did not contain classified material on its hard drive.
17	07/16/02	Boston	Bucar was burglarized.	Laptop was password protected and used to run diagnostics on radio equipment. Laptop contained classified and/or sensitive information.
18	07/17/02	Miami	Special Agent was robbed.	Laptop was used in an undercover capacity and does not contain any classified material nor any FBI macros.
19	07/29/02	FBI HQ	Special Agent's residence was burglarized.	Laptop contained classified and/or sensitive information including names, addresses and phone numbers of FBI personnel.
20	09/09/02	Indianapolis	Unable to locate during physical inventory.	CND
21	09/09/02	Indianapolis	Unable to locate during physical inventory.	Cannot Determine however laptop contained sensitive and/or classified information.
22	09/09/02	Indianapolis	Laptop never used by FBI and turned over to Supply Tech for disposal	CND
23	09/09/02	Indianapolis	Laptop never used by FBI and turned over to Supply Tech for disposal	CND
24	09/09/02	Indianapolis	Unable to locate during physical inventory-**No disciplinary action**	CND
25	09/09/02	Indianapolis	Laptop never used by FBI and turned over to Supply Tech for surplus/disposal	CND
26	10/11/02	New Orleans	Bucar was burglarized-**3-day suspension**	Laptop used for processing surveillance work.
27	10/17/02	Kansas	Laptop burglarized from rental truck	CND
28	10/18/02	New York	Laptop stolen from secure trial preparation room in USA's office	CND
29	10/25/02	New York	Bucar was burglarized	CND
30	11/05/02	New York	Unable to locate during physical inventory.	CND
31	11/05/02	New York	Unable to locate during physical inventory	Laptop used for administrative record keeping, and not investigative purposes.
32	11/12/02	New York	Unknown	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
33	11/12/02	New York	Unknown	CND
34	11/12/02	New York	Unknown	CND
35	11/12/02	New York	Unknown	CND
36	11/18/02	FBI HQ	Unknown	CND
37	11/18/02	FBI HQ	Unknown	CND
38	12/31/02	New York	Unable to locate during physical inventory	CND
39	01/08/03	Philadelphia	Special Agent lost laptop-**3-day suspension**	CND
40	02/05/03	FBI HQ	Laptop was surplused	CND
41	02/12/03	FBI HQ	Unable to locate during physical inventory	CND
42	03/07/03	Miami	Laptop burglarized from FBI boat	Laptop contained a navigation program and WordPerfect. All FBI macros had been previously removed.
43	03/31/03	FBI HQ	Unable to locate during physical inventory	CND
44	04/02/03	FBI HQ	Unknown	CND
45	05/15/03	FBI HQ	Unable to locate during physical inventory	CND
46	05/15/03	FBI HQ	Unable to locate during physical inventory	CND
47	05/27/03	Washington	Unknown	CND
48	06/09/03	New York	Unknown	CND
49	06/18/03	Atlanta	Unable to locate during physical inventory	CND
50	06/19/03	FBI HQ	Unable to locate during physical inventory	CND
51	06/25/03	Chicago	Unable to locate during physical inventory-**Letter of Censure issued**	CND
52	07/08/03	Salt Lake City	Unable to locate during physical inventory	CND
53	07/09/03	Pittsburgh	Unable to locate during physical inventory	CND
54	07/10/03	FBI HQ	Unknown	CND
55	07/14/03	San Juan	Unknown	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
56	07/14/03	FBI HQ	Laptop was stolen	CND
57	07/15/03	Philadelphia	Unable to locate during physical inventory	CND
58	07/15/03	New York	Unable to locate during physical inventory	CND
59	07/15/03	New York	Unknown	CND
60	07/15/03	Phoenix	Unable to locate during physical inventory	CND
61	07/16/03	Washington Field	Unable to locate during physical inventory	CND
62	07/16/03	Washington Field	Unable to locate during physical inventory	CND
63	07/16/03	Legal Attaché Office	Unable to locate during physical inventory	CND
64	07/16/03	Los Angeles	Unable to locate during physical inventory	CND
65	07/16/03	Boston	Unable to locate during physical inventory	CND
66	07/16/03	San Francisco	Unable to locate during physical inventory	CND
67	07/16/03	Los Angeles	Unable to locate during physical inventory	CND
68	07/16/03	Memphis	Unable to locate during physical inventory	CND
69	07/16/03	San Francisco	Unable to locate during physical inventory	CND
70	07/16/03	San Francisco	Unable to locate during physical inventory	CND
71	07/16/03	Los Angeles	Unable to locate during physical inventory	CND
72	07/16/03	FBI HQ	Unknown	CND
73	07/17/03	FBI HQ	Unknown	CND
74	07/17/03	FBI HQ	Unknown	CND
75	07/17/03	FBI HQ	Unknown	CND
76	07/17/03	FBI HQ	Unknown	CND
77	07/17/03	FBI HQ	Unknown	CND
78	07/17/03	FBI HQ	Unknown	CND
79	07/21/03	FBI HQ	Unable to locate during physical inventory—**No disciplinary action**	CND
80	07/21/03	FBI HQ	Unable to locate during physical inventory—**No disciplinary action**	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
81	07/21/03	FBI HQ	Car was burglarized	CND
82	07/21/03	FBI HQ	Unable to locate during physical inventory—**No disciplinary action**	CND
83	07/22/03	FBI HQ	Unable to locate during physical inventory	CND
84	07/23/03	FBI HQ	Unable to locate during physical inventory—**No disciplinary action**	CND
85	07/23/03	FBI HQ	Unable to locate during physical inventory-**No disciplinary action**	CND
86	09/29/03	Washington	Laptop stolen from Hotel	CND
87	10/09/03	FBI HQ	Laptop stolen from unlocked vehicle	CND
88	11/10/03	San Diego	Laptop disposed	CND
89	12/01/03	Seattle	Laptop stolen from Bucar	CND
90	01/26/04	San Francisco	Laptop stolen from POV-**No disciplinary action**	Laptop used primarily for surveillances.
91	03/18/04	Washington	Laptop stolen	Laptop contained certification and accreditation documentation.
92	03/24/04	Unknown	Unknown	CND
93	03/24/04	Information Resource Division	Unable to locate during physical inventory	CND
94	03/24/04	Information Resource Division	Unable to locate during physical inventory	CND
95	03/26/04	Los Angeles	Unable to locate during physical inventory	CND
96	03/26/04	Los Angeles	Unable to locate during physical inventory	CND
97	03/30/04	New York	Unable to locate during physical inventory	CND
98	04/28/04	FBI HQ	Unknown	CND
99	04/28/04	FBI HQ	Unknown	CND
100	04/28/04	FBI HQ	Unknown	CND
101	05/04/04	FBI HQ	Laptop stolen from POV	CND
102	05/04/04	Los Angeles	Unable to locate during physical inventory	CND
103	05/05/04	New York	Unable to locate during physical inventory	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
104	05/05/04	Atlanta	Unable to locate during physical inventory	CND
105	05/05/04	FBI HQ	Laptop lost in IRAQ	CND
106	05/05/04	Boston	Unable to locate during physical inventory	CND
107	05/05/04	FBI HQ	Unable to locate during physical inventory	CND
108	05/11/04	San Francisco	Unknown	CND
109	05/13/04	Birmingham	Laptop stolen from Special Agent's residence-**No disciplinary action**	CND
110	05/14/04	Milwaukee	Unable to locate during physical inventory	Laptops hard disk drive removed due to age prior to it being lost.
111	05/19/04	Washington	Unable to locate during physical inventory	CND
112	05/26/04	FBI HQ	Unable to locate during physical inventory	CND
113	05/26/04	FBI HQ	Unable to locate during physical inventory	CND
114	05/26/04	FBI HQ	Unable to locate during physical inventory	CND
115	05/28/04	New York	Laptop lost in the mail-**No disciplinary action**	CND
116	05/28/04	New York	Unknown	CND
117	05/28/04	New York	Unknown	CND
118	05/28/04	New York	Unknown	CND
119	06/03/04	FBI HQ	Unable to locate during physical inventory	CND
120	06/07/04	Seattle	Stolen from Bucar	Laptop contained no FBI programs or data.
121	06/07/04	Seattle	Stolen from Bucar	Laptop contained no FBI programs or data.
122	08/06/04	Atlanta	Unable to locate during physical inventory	CND
123	11/08/04	Boston	Unable to locate during physical inventory	Laptop contained software determined to be "obsolete".
124	11/15/04	FBI HQ	Laptop stolen	CND
125	11/15/04	FBI HQ	Laptop stolen	CND
126	11/16/04	Washington	Laptop stolen from residence	CND
127	12/03/04	Atlanta	Laptop stolen from residence-**Pending OPR investigation**	Laptop hard drive was "wiped clean" just prior to the theft.
128	12/16/04	San Francisco	Laptop stolen from Bucar	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
129	01/31/05	Los Angeles	Laptop stolen from residence	Laptop contained commercial off-the-shelf software and was fully encrypted and password protected with Pointsec.
130	04/08/05	Philadelphia	Unable to locate during physical inventory	CND
131	04/12/05	Detroit	Burglary of Motor home	CND
132	04/30/05	FBI HQ	Unknown	CND
133	05/04/05	FBI HQ	Unknown	CND
134	05/04/05	FBI HQ	Unknown	CND
135	05/04/05	FBI HQ	Unknown	CND
136	05/05/05	FBI HQ	Laptop left on plane	CND
137	05/05/05	Las Vegas	Unable to locate during physical inventory	CND
138	05/05/05	FBI HQ	Unknown	CND
139	05/06/05	FBI HQ	Unknown	CND
140	05/06/05	FBI HQ	Unable to locate during physical inventory- **Pending OPR investigation**	CND
141	05/06/05	Unknown	Unable to locate during physical inventory	CND
142	05/07/05	FBI HQ	Laptop stolen from vehicle	CND
143	05/09/05	FBI HQ	Unable to locate during physical inventory- **Pending OPR investigation**	CND
144	05/09/05	Salt Lake City	Unknown	CND
145	05/09/05	FBI HQ	Unknown	CND
146	05/12/05	FBI HQ	Laptop lost in IRAQ	CND
147	05/17/05	FBI HQ	Unknown	CND
148	06/23/05	Puerto Rico	Laptop stolen from Bucar- **Pending OPR investigation**	CND
149	08/26/05	FBI HQ	Laptop stolen from POV- **Pending OPR investigation**	Laptop included Pointsec encryption software. Laptop also included classified and/or sensitive information.
150	08/26/05	San Diego	Laptop stolen from Bucar- **Pending OPR investigation**	CND

NO.	FD-500 REPORT DATE	LOCATION	DESCRIPTION OF LOSS	CONTENTS OF LAPTOP ACCORDING TO FORM FD-500
151	10/19/05	FBI HQ	Unknown	CND
152	Unknown	FBI HQ	Unable to locate during physical inventory	CND
153	Unknown	FBI HQ	Unknown	CND
154	Unknown	FBI HQ	Unknown	CND
155	Unknown	FBI HQ	Unknown	CND
156	Unknown	FBI HQ	Unknown	CND
157	Unknown	FBI HQ	Unknown	CND
158	Unknown	FBI HQ	Unknown	CND
159	Unknown	FBI HQ	Unknown	CND
160	Unknown	FBI HQ	Unknown	CND

APPENDIX V

ANALYSIS OF LOST AND STOLEN WEAPONS

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or Inspection Division
1	Lost	3	YES	YES
2	Lost	**34**	**NO**	YES
3	Stolen	0	YES	YES
4	Stolen	3	YES	YES
5	Lost	**60**	**NO**	YES
6	Stolen	0	YES	YES
7	Stolen	27	**NO**	YES
8	Lost	1	YES	NO
9	Stolen	**93**	**NO**	YES
10	Stolen	**93**	**NO**	YES
11	Stolen	**93**	**NO**	YES
12	Stolen	**93**	**NO**	YES
13	Stolen	**93**	**NO**	YES
14	Stolen	**93**	**NO**	YES
15	Stolen	**93**	**NO**	YES
16	Lost	CND[84]	CND	YES
17	Stolen	**93**	**NO**	YES
18	Lost	CND	CND	NO
19	Stolen	**1161**	**NO**	YES
20	Lost	2	YES	NO
21	Lost	1	YES	YES
22	Stolen	**13**	**NO**	YES
23	Stolen	7	YES	YES
24	Stolen	7	YES	YES
25	Stolen	**17**	**NO**	NO
26	Stolen	**12**	**NO**	YES
27	Stolen	10	YES	YES
28	Stolen	1	YES	YES
29	Stolen	**204**	**NO**	YES
30	Lost	**1212**	**NO**	YES
31	Stolen	**46**	**NO**	YES
32	Stolen	9	YES	YES
33	Stolen	0	YES	YES
34	Stolen	4	YES	YES
35	Stolen	2	YES	YES
36	Lost	CND	CND	YES
37	Lost	4	YES	YES
38	Stolen	2	YES	YES
39	Lost	CND	CND	YES
40	Stolen	6	YES	YES

[84] CND = Could Not Determine. The FD-500 did not contain the date of the loss.

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or Inspection Division
41	Stolen	**38**	**NO**	YES
42	Stolen	**34**	**NO**	YES
43	Stolen	**13**	**NO**	YES
44	Stolen	9	YES	YES
45	Stolen	2	YES	YES
46	Stolen	**18**	**NO**	YES
47	Lost	4	YES	YES
48	Stolen	1	YES	YES
49	Stolen	**368**	**NO**	YES
50	Lost	**18**	**NO**	YES
51	Stolen	6	YES	YES
52	Stolen	1	YES	YES
53	Lost	0	YES	NO
54	Lost	0	YES	NO
55	Stolen	8	YES	YES
56	Stolen	CND	CND	YES
57	Stolen	CND	CND	YES
58	Stolen	**67**	**NO**	YES
59	Stolen	**329**	**NO**	YES
60	Stolen	**329**	**NO**	YES
61	Stolen	**73**	**NO**	YES
62	Lost	**197**	**NO**	NO
63	Lost	0	YES	YES
64	Lost	CND	CND	NO
65	Lost	0	YES	NO
66	Stolen	**1227**	**NO**	YES
67	Lost	4	YES	YES
68	Lost	4	YES	YES
69	Lost	4	YES	YES
70	Lost	4	YES	YES
71	Lost	4	YES	YES
72	Lost	4	YES	YES
73	Lost	4	YES	YES
74	Lost	4	YES	YES
75	Stolen	CND	CND	YES
76	Stolen	**3892**	**NO**	NO
77	Stolen	**541**	**NO**	YES
78	Lost	CND	CND	YES
79	Stolen	1	YES	YES
80	Lost	**310**	**NO**	NO
81	Lost	CND	CND	NO
82	Stolen	1	YES	YES
83	Stolen	1	YES	YES
84	Stolen	**2652**	**NO**	YES
85	Stolen	**863**	**NO**	YES
86	Lost	**448**	**NO**	NO

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or Inspection Division
87	Lost	**448**	**NO**	NO
88	Lost	**448**	**NO**	NO
89	Lost	**37**	**NO**	YES
90	Stolen	CND	CND	YES
91	Stolen	**17**	**NO**	YES
92	Stolen	7	YES	YES
93	Stolen	**89**	**NO**	NO
94	Stolen	1	YES	YES
95	Stolen	7	YES	YES
96	Stolen	**1634**	**NO**	NO
97	Stolen	3	YES	YES
98	Stolen	7	YES	YES
99	Stolen	**14**	**NO**	YES
100	Stolen	3	YES	YES
101	Stolen	8	YES	YES
102	Stolen	**4932**	**NO**	YES
103	Stolen	7	YES	YES
104	Stolen	**68**	**NO**	YES
105	Stolen	CND	CND	YES
106	Stolen	CND	CND	NO
107	Stolen	**5834**	**NO**	YES
108	Lost	CND	CND	YES
109	Lost	0	YES	YES
110	Stolen	CND	CND	NO
111	Lost	CND	CND	YES
112	Stolen	CND	CND	NO
113	Stolen	**8841**	**NO**	YES
114	Lost	CND	CND	YES
115	Lost	CND	CND	YES
116	Stolen	**45**	**NO**	YES
117	Stolen	2	YES	YES
118	Stolen	**1086**	**NO**	NO
119	Stolen	CND	CND	YES
120	Lost	0	YES	YES
121	Lost	CND	CND	NO
122	Lost	CND	CND	YES
123	Lost	CND	CND	YES
124	Stolen	**251**	**NO**	YES
125	Stolen	8	YES	YES
126	Lost	CND	CND	NO
127	Stolen	CND	CND	YES
128	Stolen	1	YES	YES
129	Stolen	CND	CND	YES
130	Stolen	**38**	**NO**	YES
131	Lost	CND	CND	NO
132	Lost	CND	CND	NO

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or Inspection Division
133	Lost	CND	CND	NO
134	Lost	CND	CND	NO
135	Lost	CND	CND	NO
136	Stolen	**1804**	**NO**	NO
137	Lost	CND	CND	NO
138	Lost	CND	CND	YES
139	Stolen	**318**	**NO**	YES
140	Lost	CND	CND	YES
141	Lost	CND	CND	YES
142	Lost	CND	CND	YES
143	Lost	CND	CND	YES
144	Lost	CND	CND	YES
145	Lost	CND	CND	YES
146	Lost	CND	CND	YES
147	Lost	CND	CND	YES
148	Lost	CND	CND	YES
149	Stolen	**5683**	**NO**	YES
150	Lost	CND	CND	YES
151	Lost	CND	CND	YES
152	Stolen	CND	CND	YES
153	Lost	CND	CND	YES
154	Stolen	CND	CND	NO
155	Lost	CND	CND	YES
156	Stolen	CND	CND	YES
157	Lost	CND	CND	YES
158	Stolen	**29**	**NO**	YES
159	Stolen	**29**	**NO**	YES
160	Stolen	CND	CND	NO

APPENDIX VI

ANALYSIS OF LOST AND STOLEN LAPTOP COMPUTERS

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or ID	CONTAINED SENSITIVE/ CLASSIFIED INFORMATION	REPORTED TO DOJ
1	Stolen	**63**	**NO**	YES	**YES**	NO
2	Stolen	5	YES	YES	NO	YES
3	Lost	**165**	**NO**	NO	CND	NO
4	Stolen	9	YES	YES	NO	YES
5	Lost	0	YES	NO	CND	NO
6	Lost	0	YES	NO	NO	NO
7	Stolen	**121**	**NO**	NO	CND	YES
8	Lost	0	YES	NO	NO	NO
9	Lost	**125**	**NO**	NO	NO	NO
10	Lost	CND	CND	NO	NO	NO
11	Lost	1	YES	NO	NO	NO
12	Lost	**11**	**NO**	NO	NO	NO
13	Lost	0	YES	NO	NO	NO
14	Lost	0	YES	NO	NO	NO
15	Lost	CND	CND	NO	NO	NO
16	Lost	CND	CND	NO	NO	NO
17	Lost	CND	CND	NO	NO	NO
18	Lost	CND	CND	NO	NO	NO
19	Lost	CND	CND	NO	NO	NO
20	Stolen	**23**	**NO**	YES	NO	NO
21	Lost	0	YES	YES	CND	NO
22	Stolen	**15**	**NO**	NO	NO	YES
23	Stolen	1	YES	YES	NO	YES
24	Stolen	**26**	**NO**	YES	NO	YES
25	Lost	**41**	**NO**	NO	NO	YES
26	Lost	**46**	**NO**	NO	NO	YES
27	Stolen	**34**	**NO**	NO	NO	YES
28	Lost	0	YES	NO	NO	NO
29	Stolen	6	YES	NO	NO	NO
30	Lost	0	YES	NO	NO	YES
31	Stolen	**93**	**NO**	NO	NO	YES
32	Stolen	2	YES	YES	NO	YES
33	Stolen	2	YES	NO	NO	YES
34	Lost	0	YES	NO	NO	NO
35	Lost	1	YES	NO	NO	NO
36	Lost	0	YES	NO	NO	NO
37	Lost	0	YES	NO	NO	NO
38	Stolen	**47**	**NO**	NO	NO	YES
39	Lost	CND	CND	NO	CND	NO
40	Lost	CND	CND	NO	CND	NO
41	Lost	CND	CND	NO	CND	NO
42	Lost	0	YES	NO	CND	YES

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or ID	CONTAINED SENSITIVE/ CLASSIFIED INFORMATION	REPORTED TO DOJ
43	Lost	0	YES	NO	CND	NO
44	Lost	0	YES	NO	CND	NO
45	Lost	0	YES	NO	CND	NO
46	Lost	CND	CND	NO	CND	NO
47	Lost	CND	CND	NO	CND	NO
48	Lost	CND	CND	NO	CND	NO
49	Lost	CND	CND	NO	NO	NO
50	Lost	**68**	**NO**	YES	NO	NO
51	Stolen	**959**	**NO**	NO	CND	YES
52	Lost	0	YES	NO	**YES**	NO
53	Lost	**817**	**NO**	NO	NO	NO
54	Lost	CND	CND	NO	CND	NO
55	Lost	**300**	**NO**	NO	NO	YES
56	Lost	0	YES	NO	CND	NO
57	Lost	**71**	**NO**	YES	NO	NO
58	Lost	0	YES	NO	NO	NO
59	Lost	CND	CND	NO	NO	NO
60	Stolen	**30**	**NO**	NO	NO	YES
61	Lost	CND	CND	NO	CND	YES
62	Lost	**461**	**NO**	NO	CND	YES
63	Lost	**776**	**NO**	NO	CND	YES
64	Lost	**776**	**NO**	NO	CND	YES
65	Lost	**776**	**NO**	NO	CND	YES
66	Lost	**696**	**NO**	NO	CND	YES
67	Lost	**527**	**NO**	NO	CND	YES
68	Lost	**1862**	**NO**	NO	NO	YES
69	Stolen	7	YES	NO	**YES**	YES
70	Lost	CND	CND	YES	CND	YES
71	Lost	7	YES	NO	CND	YES
72	Stolen	**19**	**NO**	NO	NO	YES
73	Lost	**68**	**NO**	NO	NO	YES
74	Lost	**68**	**NO**	NO	NO	YES
75	Lost	CND	CND	NO	CND	YES
76	Stolen	**25**	**NO**	NO	NO	YES
77	Lost	CND	CND	NO	NO	YES
78	Stolen	CND	CND	NO	NO	YES
79	Lost	CND	CND	NO	CND	NO
80	Lost	CND	CND	NO	CND	YES
81	Lost	0	YES	NO	NO	YES
82	Lost	CND	CND	NO	CND	NO
83	Lost	0	YES	YES	CND	NO
84	Lost	CND	CND	YES	CND	NO
85	Lost	CND	CND	YES	CND	NO
86	Lost	CND	CND	YES	CND	NO
87	Stolen	**269**	**NO**	NO	NO	YES
88	Lost	0	YES	YES	CND	NO

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or ID	CONTAINED SENSITIVE/ CLASSIFIED INFORMATION	REPORTED TO DOJ
89	Lost	0	YES	NO	NO	NO
90	Lost	0	YES	NO	CND	YES
91	Lost	0	YES	YES	CND	NO
92	Lost	CND	CND	NO	NO	YES
93	Lost	CND	CND	NO	CND	NO
94	Lost	**60**	**NO**	NO	CND	NO
95	Lost	CND	CND	NO	NO	YES
96	Lost	0	YES	NO	NO	NO
97	Stolen	CND	CND	NO	NO	YES
98	Stolen	CND	CND	NO	**YES**	YES
99	Lost	0	YES	NO	NO	NO
100	Lost	0	YES	NO	NO	NO
101	Lost	CND	CND	YES	NO	NO
102	Lost	0	YES	NO	NO	YES
103	Lost	0	YES	NO	NO	NO
104	Stolen	**40**	**NO**	YES	CND	YES
105	Lost	6	YES	NO	NO	NO
106	Stolen	**693**	**NO**	YES	NO	YES
107	Lost	0	YES	YES	NO	NO
108	Lost	CND	CND	YES	CND	NO
109	Lost	0	YES	NO	NO	NO
110	Lost	CND	CND	NO	NO	YES
111	Lost	0	YES	YES	**YES**	NO
112	Lost	CND	CND	NO	NO	YES
113	Lost	CND	CND	YES	**YES**	YES
114	Lost	CND	CND	NO	NO	YES
115	Lost	CND	CND	NO	CND	YES
116	Lost	**234**	**NO**	YES	NO	YES
117	Stolen	CND	CND	YES	CND	YES
118	Lost	CND	CND	YES	NO	YES
119	Lost	CND	CND	NO	NO	YES
120	Lost	CND	CND	NO	CND	YES
121	Lost	CND	CND	NO	CND	YES
122	Stolen	**1821**	**NO**	NO	NO	YES
123	Lost	CND	CND	NO	NO	YES
124	Lost	3	YES	NO	CND	YES
125	Stolen	**17**	**NO**	YES	**YES**	YES
126	Lost	CND	CND	NO	NO	YES
127	Lost	CND	CND	YES	CND	YES
128	Lost	CND	CND	YES	NO	YES
129	Lost	CND	CND	NO	NO	NO
130	Lost	CND	CND	NO	NO	NO
131	Lost	CND	CND	NO	NO	NO
132	Lost	CND	CND	NO	NO	NO
133	Lost	CND	CND	NO	NO	NO
134	Lost	CND	CND	NO	NO	NO

NUMBER	LOSS TYPE	DAYS BETWEEN LOSS AND FD-500 SUBMITTED	FD-500 TIMELY	REFERRED TO FBI'S OPR or ID	CONTAINED SENSITIVE/ CLASSIFIED INFORMATION	REPORTED TO DOJ
135	Stolen	CND	CND	NO	NO	NO
136	Stolen	CND	CND	NO	NO	NO
137	Stolen	CND	CND	YES	NO	NO
138	Lost	CND	CND	NO	NO	NO
139	Lost	CND	CND	NO	NO	NO
140	Lost	CND	CND	NO	NO	NO
141	Lost	CND	CND	NO	NO	NO
142	Stolen	CND	CND	NO	NO	NO
143	Stolen	CND	CND	NO	CND	NO
144	Stolen	CND	CND	NO	NO	NO
145	Stolen	**1216**	**NO**	YES	NO	NO
146	Stolen	CND	CND	NO	NO	NO
147	Stolen	CND	CND	YES	NO	NO
148	Stolen	CND	CND	NO	NO	NO
149	Stolen	CND	CND	NO	NO	NO
150	Stolen	CND	CND	NO	NO	NO
151	Stolen	CND	CND	NO	NO	NO
152	Stolen	CND	CND	NO	NO	NO
153	Lost	CND	CND	YES	NO	NO
154	Lost	CND	CND	NO	CND	NO
155	Stolen	CND	CND	NO	NO	NO
156	Lost	CND	CND	NO	NO	NO
157	Lost	CND	CND	YES	NO	NO
158	Lost	CND	CND	YES	CND	NO
159	Lost	CND	CND	YES	NO	NO
160	Stolen	CND	CND	YES	CND	NO

APPENDIX VII

ANALYSIS OF THE 51 LOST AND STOLEN LAPTOP COMPUTERS THAT FBI DID NOT KNOW IF THEY CONTAINED SENSITIVE OR CLASSIFIED INFORMATION

NO.	FD-500 REPORT DATE	TYPE OF LOSS	DATE OF LOSS	LAPTOP ASSIGNED TO AN INDIVIDUAL	CIRCUMSTANCES OF LOSS	FIELD OFFICE OR DIVISION
1	10/25/2001	stolen	unknown	No	Office space was burglarized	Baltimore
2	12/6/2001	lost	unknown	No	during physical inventory	Cyber Division
3	1/25/2002	stolen	unknown	Yes	FBI car burglarized	New York
4	3/12/2002	lost	unknown	No	during physical inventory	CIRG Rapid Deployment Unit
5	7/17/2002	stolen	unknown	Yes	laptop stolen from Task Force Detective	Miami
6	1/8/2003	lost	unknown	Yes	unknown	Philadelphia
7	3/31/2003	lost	3/28/2003	No	during physical inventory	Information Resource Div
8	5/27/2003	stolen	10/10/2000	Yes	unknown	Washington
9	6/19/2003	lost	unknown	No	during physical inventory	Information Resource Div
10	6/25/2003	stolen	05/16/2003	Yes	during physical inventory	Chicago
11	7/9/2003	lost	7/09/2003	No	during physical inventory	Pittsburgh
12	7/15/2003	lost	7/15/2003	No	during physical inventory	New York
13	7/16/2003	lost	unknown	Yes	during physical inventory	Washington
14	7/16/2003	lost	unknown	No	during physical inventory	Washington
15	7/16/2003	lost	unknown	Yes	during physical inventory	Legat Nairobi
16	7/16/2003	lost	5/17/2003	Yes	during physical inventory	Los Angeles
17	7/17/2003	lost	4/12/2002	No	unknown	Counter-Intelligence Division
18	7/17/2003	lost	6/01/2001	No	unknown	Counter-Intelligence Division
19	7/17/2003	lost	6/01/2001	No	unknown	Counter-Intelligence Division

NO.	FD-500 REPORT DATE	TYPE OF LOSS	DATE OF LOSS	LAPTOP ASSIGNED TO AN INDIVIDUAL	CIRCUMSTANCES OF LOSS	FIELD OFFICE OR DIVISION
20	7/17/2003	lost	6/01/2001	No	unknown	Counter-Intelligence Division
21	7/17/2003	lost	8/20/2001	No	unknown	Counter-Intelligence Division
22	7/17/2003	lost	2/05/2002	No	unknown	Counter-Intelligence Division
23	7/21/2003	lost	7/21/2003	No	during physical inventory	Cyber Division
24	7/21/2003	lost	unknown	No	during physical inventory	Cyber Division
25	7/21/2003	lost	7/21/2003	No	during physical inventory	Cyber Division
26	7/23/2003	lost	unknown	No	during physical inventory	Cyber Division
27	7/23/2003	lost	unknown	No	during physical inventory	Cyber Division
28	3/26/2004	lost	unknown	No	during physical inventory	Los Angeles
29	3/26/2004	lost	3/19/2004	No	during physical inventory	Los Angeles
30	4/28/2004	lost	unknown	No	unknown	ITD,TPS,Technical Personnel Dev
31	4/28/2004	lost	unknown	No	unknown	ITD,TPS,Technical Personnel Dev
32	4/28/2004	lost	unknown	No	unknown	ITD,TPS,Technical Personnel Dev
33	5/4/2004	lost	5/4/2004	Yes	during physical inventory	Los Angeles
34	5/5/2004	lost	unknown	No	during physical inventory	Atlanta
35	5/28/2004	lost	5/28/2004	Yes	laptop lost in the mail	New York
36	5/28/2004	lost	5/28/2004	No	unknown	New York
37	5/28/2004	lost	5/28/2004	No	unknown	New York
38	5/28/2004	lost	5/28/2004	No	unknown	New York
39	4/8/2005	lost	4/08/2005	Yes	unknown	Philadelphia
40	5/6/2005	lost	11/22/2004	No	Unknown	Security Division
41	5/7/2005	stolen	1/06/2005	No	stolen from vehicle	Cyber Division
42	5/17/2005	lost	5/17/2005	No	Unknown	Office of International Operations
43	Unknown	lost	unknown	No	during physical inventory	Counterterrorism Div

NO.	FD-500 REPORT DATE	TYPE OF LOSS	DATE OF LOSS	LAPTOP ASSIGNED TO AN INDIVIDUAL	CIRCUMSTANCES OF LOSS	FIELD OFFICE OR DIVISION
44	No-FD-500	unk	unknown	No	unknown	Baltimore-Special Ops Group
45	No-FD-500	unk	unknown	No	unknown	Cyber Division
46	No-FD-500	unk	unknown	No	unknown	New York
47	No-FD-500	unk	unknown	No	unknown	CIRG Rapid Deployment Unit
48	No-FD-500	unk	unknown	No	unknown	Miami
49	No-FD-500	unk	unknown	No	unknown	Philadelphia
50	No-FD-500	unk	unknown	No	unknown	Information Resource Div
51	No-FD-500	unk	unknown	No	unknown	Washington Field Office

APPENDIX VIII

ANALYSIS OF PROPERTY MANAGEMENT RECORDS

Table 1: FBI UNIVERSE OF FBI WEAPONS

Field Name	Data Type	Non blank	Blank	Total
COST CODE	Code number	52,263	0	52,263
COST CENTER NAME	Location	52,003	260	52,263
BAR CODE	Bar code	52,263	0	52,263
SERIAL NUMBER	Serial number	52,224	39	52,263
MANUFACTURER	Name	52,263	0	52,263
MODEL NUMBER	Model number	52,263	0	52,263
DESCRIPTION	Description	52,263	0	52,263
AGENT ASSIGNED	Name of Agent	12,138	40,125 [85]	52,263

Table 2: FBI UNIVERSE OF LAPTOPS

Field Name	Data Type	Non blank	Blank	Total
COST CODE	Code number	25,302	864	26,166
COST CENTER NAME	Location	25,195	971	26,166
BAR CODE	Bar code	26,166	0	26,166
SERIAL NUMBER	Serial number	26,074	92	26,166
MANUFACTURER	Name	26,166	0	26,166
MODEL NUMBER	Model number	26,128	38	26,166
DESCRIPTION	Description	26,166	0	26,166
AGENT ASSIGNED	Name of Agent	15,742	10,424	26,166

[85] The weapons that were not assigned to individuals were either vault weapons or training weapons for which all had a cost code assigned.

APPENDIX IX

LOST AND STOLEN FBI WEAPONS NOT FOUND IN NCIC

NUMBER	BARCODE	MAKE	MODEL
1	F1540624	GLOCK	22
2	F1467970	GLOCK	22
3	F1822816	GLOCK	22
4	F1017831	GLOCK	22
5	F1921421	GLOCK	22
6	F1389423	GLOCK	22
7	F0308929	SIG SAUER	P226 AUTO
8	F1540157	GLOCK	22
9	F1111189	SIG SAUER	P226 AUTO
10	U447328	REMINGTON	870
11	F0436721	S & W	13
12	F0010500	COLT	N/A
13	F1048448	GLOCK	22
14	F1388886	GLOCK	22
15	F1091373	S & W	10
16	F0647530	S & W	19
17	F1092647	S & W	13
18	F0648546	S & W	27
19	F1092868	S & W	10
20	F1092953	S & W	10
21	F1093198	S & W	10
22	F1092532	S & W	10
23	F1092048	S & W	19

APPENDIX X

LOST AND STOLEN LAPTOP COMPUTERS NOT FOUND IN NCIC

NUMBER	BARCODE	SERIAL NUMBER	MANUFACTURER
1	F1472532	BDB31400305	DELL
2	F1247697	P01061000250062	IDP
3	F1458830	78-BMZT5	IBM
4	F1848225	78-KYGMZ	IBM
5	F1400248	KP-BPKLL	IBM
6	F2120756	KLRF	IBM
7	F1424477	AF-1BWFK	IBM
8	F1929724	KPYMRZD	IBM
9	F1289770	78-VHFR1	IBM
10	F1384882	78-X61190998	IBM
11	F1551015	78RL664	IBM
12	F1918255	3573365-0001	MPC
13	F0979096	35662580001	MICRON
14	F2085722	KP7T6P5	IBM
15	F0793230	3562637	MICRON
16	F1140937	NC3-8812	DGI
17	F1915877	4EKSB06698	PANASONIC
18	F0967142	283094313928924	SONY
19	F0967346	S014004637A	SONY
20	F1247637	P01061000250002	IDP
21	F1289772	78-VHCP6	IBM
22	F1842502	78C4498	IBM
23	F1842504	78C0564	IBM
24	F1071683	78CCRFH	IBM
25	F1802804	XB235008N6A	APPLE
26	F1802813	XB236025N6A	APPLE
27	F1802814	XB23701EN6A	APPLE
28	F1150487	P00589500100143	IDP
29	F1516573	AF-1BTLN	IBM
30	F1516608	AF-1BW2X	IBM
31	F1516609	AF-1BW9A	IBM
32	F1929565	KPZLHLR	IBM
33	F1929573	KPZLHHL	IBM
34	F1929607	KPZLHKN	IBM
35	F0155722	NC35345	IDP
36	F0441398	16206410099	MICRON
37	F1854595		TOSHIBA
38	F0765954	94390743	DELL
39	F1000426	FC5039HV49G	POWERBOOK
40	F1424484	AF-1BWBF	IBM

NUMBER	BARCODE	SERIAL NUMBER	MANUFACTURER
41	F1445033	23DPR69	IBM
42	F1703658	99TF0N7	IBM
43	F1282091	0020060393	GATEWAY
44	F0441399	16206410100	MICRON
45	F1424571	19425040001	MICRON
46	F1424574	19424970001	MICRON
47	F1424575	19424980001	MICRON
48	F1424744	24238550001	MICRON
49	F1424753	24238190001	MICRON
50	F1424778	24238600001	MICRON
51	F1425546	78CX737	IBM
52	F1929697	3IKSA10150	PANASONIC
53	F1779003	0032502807	GATEWAY
54	F1779004	0032502808	GATEWAY
55	F1641969	1753D11	DELL
56	F0441313	16206410014	MICRON
57	F0441396	16206410097	MICRON
58	F1420033	0015828768	GATEWAY
59	F1528930	78RG369	IBM
60	F1583663	78MRFAC	IBM
61	F1289768	78-VHCB1	IBM
62	F1280968	1V92CGX5W0YP	COMPAQ
63	F0577096	R16760	GRID SYSTEMS
64	F0655063	S3N0007A	COMPAQ
65	F0364358	264795U	IBM
66	F1171505	78RTY999608	IBM
67	F1171560	78RTY499609	IBM
68	F1176889	78RPL259608	IBM
69	F1506740	78-NKXH10800	IBM
70	F1506762	78-AL3050900	IBM
71	F0656045	6542HFJ6D307	COMPAQ
72	F1053739	A3849C0500527	OLIVETTI ECHOS PENTIUM 100
73	F1171563	78RTX00	IBM
74	F1121717	78BNAA9	IBM
75	F1072624	TE0134700497	HITACHI
76	F1385242	78-LCHY3	IBM
77	F1511025	1CYUA1218	PANASONIC
78	F1767062	0026316401	GATEWAY
79	F1207909	78-C0490	IBM
80	F1209239	0013922597	GATEWAY
81	F1528798	78RH162	IBM
82	F1246275	0019436028	GATEWAY
83	F1726551	ZZGEG2330ZZ4666	ITRONIX

NUMBER	BARCODE	SERIAL NUMBER	MANUFACTURER
84	F0441220	0011071112	GATEWAY
85	F1142385	NCP02636	DGI
86	F1162229	23-786HZ	IBM
87	F1208504	P00710000100008	IBM
88	F0573839	T2043	GRID SYSTEMS
89	F1171583	78RRW849609	IBM
90	F1767089	0499104029	KDS
91	F1149860	P00685600100007	IDP
92	F1148322	P00394600100046	IDP
93	F1383981	N8009F5P03564	IMPERIAL
94	F1084564	78ALCF4	IBM
95	F1148649	P00418600100006	IDP
96	F1142457	P00354000100004	IDP
97	F1148154	P003540000100016	IDP
98	F0704189	7525624	TOSHIBA
99	F1151050	F00820100100002	IDP
100	F1534539	AAD9B81	IBM
101	F0626413	0020060428	GATEWAY
102	F1076633	P00525000150001	NOTEBOOK
103	F1151013	P0086300010024	IEP
104	F1152016	P00895100100036	IDP
105	F0447778	4379310786	TEXAS INSTRUMENTS
106	F0727397	NC35030	IDP
107	F1140751	NC38111	IDP
108	F1152243	P00886400100043	IDP
109	F1516535	AF-1BWAW	
110	F1561802	3003659-0001	MICRON
111	F1354993	0015099887	GATEWAY
112	F1140788	NC38148	IDP
113	F1141008	38247	IDP
114	F0299933	130DE016018	ZENITH
115	F0299934	130DE01585	ZENITH
116	F0299935	130DE015588	ZENITH
117	F1425523	78CR175	IBM
118	F0704426	78TLMFG	IBM
119	F1445837	6D14JC5EBO-GP	PRESARIO
120	F0287818	30036830001	MICRON
121	F1122135	BC899380151	GATEWAY 2000
122	F1459801	AF1BW1N	IBM
123	F0552033	78ARKK6	IBM
124	F1022368	78AN425	IBM
125	F1516627	AF-1BTH6	IBM
126	F0897901	GZY092400337	MICRON

NUMBER	BARCODE	SERIAL NUMBER	MANUFACTURER
127	F1020901	78FVBVV	IBM
128	F1147534	P00310300350034	DGI
129	F1149333	P00559100150033	IDP
130	F1170016	78-BBF72	IBM
131	F1207747	78-CX559	IBM
132	F1271603	78-MAMR3	IBM
133	F1247716	P01061000250087	IDP
134	F1516843	AF-1BWCX	IBM
135	F1141346	NC313106	IDP
136	F1393739	78-CV095	IBM

APPENDIX XI

LOST OR STOLEN WEAPONS AND LAPTOPS BY FBI FIELD OFFICE

FIELD OFFICE	WEAPONS	LAPTOPS
Albany, NY	6	0
Albuquerque, NM	5	0
Atlanta, GA	9	4
Baltimore, MD	1	1
Birmingham, AL	1	1
Boston, MA	6	4
Charlotte, NC	1	0
Chicago, IL	2	1
Cleveland, OH	2	0
Columbia, SC	1	0
Dallas, TX	5	0
Denver, CO	1	0
Detroit, MI	1	1
El Paso, TX	2	0
Honolulu, HI	1	0
Houston, TX	3	0
Indianapolis, IN	1	6
Jackson, MS	1	0
Jacksonville, FL	1	0
Kansas, KS	0	2
Knoxville, TN	1	0
Las Vegas, NV	0	1
Little Rock, AR	1	0
Los Angeles, CA	8	9
Memphis, TN	0	1
Miami, FL	7	3
Michigan, MI	1	0
Milwaukee, WI	2	1
Minneapolis, MN	1	0
Mobile, AL	8	0
New Orleans, LA	2	1
New York, NY	13	18
Oklahoma City, OK	4	0
Omaha, NE	3	0
Philadelphia, PA	3	4
Phoenix, AZ	3	1
Pittsburg, PA	1	1
Providence, RI	0	0
Richmond, VA	4	0
Sacramento, CA	2	0
Salt Lake City, UT	7	4
San Antonio, TX	3	1
San Diego, CA	1	2
San Francisco, CA	4	6
San Juan, PR	4	3
Seattle, WA	2	3
Tampa, FL	3	0
Unknown	11	10
Washington DC	11	8
FBI Headquarters	0	63
TOTAL	**160**	**160**

REVISED FORM FD-500

FD-500 (Rev. 7-24-02)

FEDERAL BUREAU OF INVESTIGATION
REPORT OF LOST OR STOLEN PROPERTY
PROPERTY MANAGEMENT MATTERS

This form is to be submitted to the Property Management Unit within 10 days from the date of loss or theft.

Date:

To:

From:

Reported by: Cost Center:

Circumstances: ☐ Stolen ☐ Lost ☐ Other _____

Date of Loss/Theft _____

Description: _____

Asset Classification: _____ Acquisition Cost: _____

Manufacturer: _____ Serial Number: _____

Model Number: _____ Asset Number: _____

☐ Confidential Property: ☐ Non-confidential Property

Did this item contain sensitive/classified information? ☐ Yes ☐ No
(If "yes," attach required information. See MIOG, Part II, Section 26-13.1.)

Has this item been entered into NCIC? (If "no," please explain on attachment.) ☐ Yes ☐ No

Date entered into NCIC _____ NIC# _____

Has administrative action been taken regarding this matter? ☐ Yes ☐ No

Have you advised the FBIHQ Security Division? ☐ Yes ☐ No

Have you forward a copy of this report to OPR? ☐ Yes ☐ No

Property was last assigned/charged-out to: _____

Property custodian responsible for physical custody: _____

Details or explanation regarding the circumstances of this report:
(Continued on separate sheet if necessary):

Recommendation of Accountable Property Officer (APO):

_____ _____
Signature of APO Signature of Supply Technician

FORM FD-281

FD-281 (Rev. 7-25-02)

RECEIPT FOR GOVERNMENT PROPERTY
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE

Date: _____

I certify that I have received and/or returned the government property acknowledged below for official use:

RECEIVED: ☐

FBI Identification Card No. _____
Special Agent Badge No. _____
Special Agent Credential Card No. _____
Support Employee Credential Card No. _____
Contractor/Task Force/Other Credential Card No. _____
Key No. _____ Hook No. _____ Room No. _____
Government Credit Card No. _____
Telephone Calling Card No. _____
Cellular Telephone No. _____
Laptop Computer No. _____
Bullet Proof Vest _____
Other _____

Property Received From: _____ _____ _____
(Signature) (Typed Name) (Date)

_____
(Signature)

_____
(Typed Name)

_____
(SSN)

RETURNED ☐

Reason for Returning: ☐ Absence for Maternity Reasons ☐ Transfer ☐ Military Leave ☐ Resignation ☐ Retiring ☐ Other

FBI Identification Card No. _____
Special Agent Badge No. _____
Special Agent Credential Card No. _____
Support Employee Credential Card No. _____
Contractor/Task Force/Other Credential Card No. _____
Key No. _____ Hook No. _____ Room No. _____
Government Credit Card No. _____
Telephone Calling Card No. _____
Cellular Telephone No. _____
Laptop Computer No. _____
Bullet Proof Vest _____
Other _____

Property Returned To: _____ _____ _____
(Signature) (Typed Name) (Date)

The government property which you hereby acknowledge is charged to you and you are responsible for taking care of it and returning it when its use has been completed. **Employee will be required to reimburse the FBI for lost/stolen property in cases where the employee is found to be negligent.**

_____
(Signature)

_____
(Typed Name)

_____
(SSN)

FORM FD-519

FD-519 (Rev. 7-12-84)

REQUIREMENTS AND CERTIFICATION FOR CANNIBALIZATION AND DESTRUCTION OF EQUIPMENT

REQUIREMENTS

After Bureau authority is granted cannibalization and destruction of equipment for the purpose of obtaining parts to repair a like item is permitted when all of the following conditions are met:

1. Repair of broken or worn parts is not possible.
2. Required parts are not available from other units previously cannibalized.
3. Required parts are not available from Government excess. (Government excess means any personal property under the control of any Federal Agency which is not required for its needs to the discharge of its responsibilities, as determined by the head thereof)
4. The parts are not available from commercial or Government supply sources or it is not practical to obtain the required parts from commercial sources because of obsolescence, excessive price or extraordinary lead times.
5. The benefit realized from cannibalization exceeds the estimated trade-in or sale value of the unit being considered for cannibalization.
6. A signed statement, approved by a reviewing official, indicating the actions taken to verify the above conditions is made part of the file supporting the removal of the cannibalized item from property records, and such information is made available upon request to General Accounting Office and Department auditors.
7. In accordance with General Services Administration authorization, dated _____ .

CERTIFICATION

In conditions, as set forth above have been made to the best of my knowledge with regard to the equipment listed below and on FD-508, SF-126, or SF-120, Number _____ , dated _____ . This equipment should therefore be removed from inventory and the parts will be used for the repair and maintenance of similar equipment.

Name	
Position Title	
Office	Date
Reviewed by	

Item Description
Property Number
Serial Number

FORM FD-193

FD-193 (Rev. 12-5-02)
Report of Exit and Separation

To: Date:

From:

Name of Employee | EOD Date | Title

Cease-active-duty Date (hour and last day physically at work) | Working Hours (include workweek if other than Monday-Friday)

Interview Conducted By: (Signature) | Title:

Read Before Interviewing
Purposes: Serves as a basis for (1) information supplied by Bureau upon request by State Unemployment Compensation Boards, (2) accurate analysis of turnover, (3) determining necessary or desirable organizational improvements, and (4) permitting a recorded recommendation regarding future reinstatement (5) and ensuring the return of government property.
When and Where Conducted: As promptly as possible after receipt of resignation in adequate privacy with adequate time.
Reasons Given for Separation: The reason that the employee documented on the SF-52, and the electronic entry of same into BPMS, should be placed in only one corresponding category of reason.

01 ☐ Resignation
Retirements:
02 ☐ Optional
03 ☐ Mandatory
04 ☐ Disability
05 ☐ Discontinued Service
06 ☐ Military
07 ☐ Maternity
08 ☐ Reduction-in-Force (RIF)
09 ☐ Other Federal Agency (Complete A listed below)
10 ☐ Removal
11 ☐ Other _____

A. Comments: If employee is transferring to another federal government agency, state what agency transferring to, the address, and when employment will begin on the back of the form SF-52, Request for Personnel Action.

B. Employee was advised by interviewing official that employment information beyond name, past and present positions, titles, grades, salaries, duty stations, and reason for separation as shown on the Notification of Personnel Action may be disseminated if a prospective employer is a Federal Agency or a state or local agency within the criminal justice community, without the written consent of the employee. ☐ Yes ☐ No

C. 1. Did employee violate terms under transfer agreement, 3-34b ☐ Yes ☐ No; Foreign Assignment, FD-382 ☐ Yes ☐ No; Government Employees' Training Act ☐ Yes ☐ No; Transportation Expense Agreement, 3-591? ☐ Yes ☐ No
2. Did employee resign prior to expiration of any agreement made not covered in #1, such as to remain a specific period following initial appointment or following special training? ☐ Yes ☐ No If yes, specify agreement(s) involved and explain.
3. If support employee, did employee resign within 182 days of entrance on duty owing advanced salary? ☐ Yes ☐ No
4. If answer to either question 1, 2, or 3 above is "Yes" and/or employee has advanced leave:
a. ☐ Will the employee be indebted to the U.S. government? ☐ Yes ☐ No If yes: How does employee intend to discharge this debt?
_____
b. ☐ Advise employee that interest can be charged on overdue payments at the current Treasury rate.
c. ☐ Advise employee any money due will be held in abeyance until determination is made as to any indebtedness.

D. Employee has been advised concerning Post-Employment Restrictions in the Ethics Reform Act of 1989, as detailed in Part I, Section 1-1 (11) of the Manual of Administrative Operations and Procedures. ☐ Yes ☐ No (If No, explain why.)

E. Employee has been afforded a debriefing by his/her respective Security Officer. ☐ Yes ☐ No (If No, explain why.)

F. All documents made or received while in the FBI's service will be collected on date employee ceases active duty (exceptions: Commendations, censure or promotion letters or copies of expense vouchers, etc.) ☐ Yes ☐ No

G. If employee is resigning for maternity purposes, appropriate block must be marked:
☐ Even though the employee may be incapacitated for duty following the cease-active-duty date, she is not entitled to a lump sum payment for sick leave.
☐ Doctor's certificate attached indicating (1) employee is incapacitated for duty after indicated cease-active-duty date, and (2) expected date of confinement.
☐ Doctor's certificate attached indicating employee can safely continue working until date specified. (Applicable to those cases where the employee desires to work up to less than 6 weeks before expected date of delivery.)

H. Was employee advised that any inquires concerning his/her FBI employment should be directed to FBI, JEH Building, 935 Pennsylvania Ave., N. W. Washington, D.C. 20535, as such information is not available elsewhere? ☐ Yes ☐ No

I. Was retiring employee (including approved disability retirements) advised that his/her credentials/identification card and SA badge will be mounted on a retirement plaque and forwarded to him/her? ☐ Yes ☐ No Property to be mounted on the plaque should be forwarded to FBIHQ, Retirement Office, Room 1829.

ABBREVIATIONS AND FORMS

Abbreviations:

ATF	Bureau of Alcohol, Tobacco, and Firearms
AMU	Asset Management Unit
APO	Accountable Property Officer
BUCAR	Bureau (FBI) car
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services Division
DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Response Team
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINET	FBI Secure Network
FTU	Firearms Training Unit
MAOP	Manual of Administrative Operations and Procedures
MIOG	Manual of Investigative Operations and Guidelines
NCIC	National Crime Information Center
NSI	National Security Information
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPR	Office of Professional Responsibility
PED	Portable Electronic Device
PFI	Principal Firearms Instructor
PMA	Property Management Application
PMO	Property Management Officer
POV	Privately Owned Vehicle
SAC	Special Agent in Charge
SCI	Sensitive Compartmented Information
SCU	Security Compliance Unit
SEPS	Security and Emergency Planning Staff
SPM	Security Programs Manager
US-CERT	United States Computer Emergency Readiness Team

Forms:

FD-193 - Report of Exit and Separation
FD-281 - Report of Government Property
FD-500 - Report of Lost or Stolen Property – Property Management Matters
FD-519 - Requirements And Certification For Cannibalization And Destruction of Equipment

NATIONAL SECURITY INFORMATION

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 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 (U.S. Department of Justice, Security and Emergency Planning Staff, Classified National Security Information: Reference Booklet, June 1998, pp. 1 and 3).

AUDITEE RESPONSE

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

January 18, 2007

Mr. Guy K. Zimmerman
Assistant Inspector General for Audit
U.S. Department of Justice
Office of the Inspector General
Washington, D.C.

Re: OIG's Draft Audit Report The Federal Bureau of Investigation's Control over Weapons and Laptops Follow-Up Audit

Dear Mr. Zimmerman:

The FBI appreciates the opportunity to respond to findings and recommendations made in your report entitled "The Federal Bureau of Investigation's Control over Weapons and Laptops Follow-Up Audit" (hereinafter "Report").

Your transmittal memorandum requested the FBI provide comments on the recommendations set forth in the Report. This letter will convey the FBI's response to each of the recommendations and I request that it be appended to the Report.

The Report concludes that "the FBI has made progress in decreasing the rate of loss for weapons and laptops" and notes the positive trend in this direction since our implementation of corrective action policies in 2002. This progress reflects the FBI's commitment to minimizing such losses. Data contained in the Report reflects a 349% reduction in the average number of weapons lost or stolen in any given month when compared to data in your 2002 report. A similar reduction of 312% was reported for lost or stolen laptop computers. The Report further notes "we recognize that in an organization the size of the FBI, some weapons and laptops will inevitably be stolen or go missing." We believe we have taken and continue to take appropriate steps to minimize these losses. The data in the Report supports this position.

The FBI objects, however, to certain conclusions and negative inferences made in the Report based on the inclusion of specific data related to the overall number of weapons reported as lost during the audit period. Overall, 160 weapons were reported as lost or stolen during the most recent audit period. The FBI detailed for the OIG auditors that 43 of the 160 weapons were, in fact, lost or stolen during the *prior audit period* and were reported during the current audit period as a result of corrective actions taken to comply with the 2002 audit report. The actual number of weapons lost or stolen during the most recent 44 months, the current audit period, total 117. The FBI's objection was noted in footnote 8 of the Report along with justification provided by the OIG for including the 43 weapons in the Report's current loss calculations. We respectfully disagree with the justification provided and strongly believe the inclusion of the 43 weapons inaccurately reflects the results of continuing improvements made by the FBI in safeguarding its weapons inventory.

We acknowledge that more needs to be done to ensure the proper handling of the loss and theft of laptop computers and, more importantly, the information maintained thereon. One of the most important steps taken requires the encryption and password protection of all FBI laptop computers. As set forth by the Security Division in a Security Bulletin dated July 14, 2006, all FBI laptops must have basic configurations which include encryption to protect Sensitive but Unclassified information such as Personally Identifying Information (PII). This specific Security Bulletin contains a total of nine requirements and recommendations designed to minimize the potential for loss of FBI laptops and information. Additional policies related to the protection of not only PII information but also all other classifications of National Security related information were promulgated in April 2006 in the FBI's comprehensive Security Policy Manual.

Our continued commitment to strengthen our response to and internal control over the loss and theft of weapons and laptop computers is found in our response to the Report's recommendations. Overall, the Report identified 13 recommendations. The FBI concurs with 12 of the recommendations and offers an alternative action plan for one.

Individual recommendations and our respective responses are set forth below:

Response to Weapon and Laptop Losses

1. **OIG Recommendation:** Ensure that the Asset Management Unit (AMU) maintains all Form FD-500s with accompanying documentation and required information.

The FBI agrees with the OIG recommendation. As of October 1, 2006 the AMU began scanning and electronically maintaining all Form FD-500s and accompanying information received. As resources permit, all previously submitted and processed Form FD-500s will be scanned for electronic retention purposes.

2. **Recommendation:** Ensure that the most current version of the Form FD-500 is used to report weapon and laptop losses.

The FBI agrees with the OIG recommendation. On October 1, 2006 the AMU began conducting preliminary reviews of each submitted Form FD-500. Since that date, any submission found to have been made on an outdated form is returned for correction and proper submission.

3. **Recommendation:** Ensure that all Form FD-500s that are submitted to the Asset Management Unit are complete, accurate and timely. Specifically, the FBI should ensure that the contents of the lost or stolen laptop computers accompany the Form FD-500.

The FBI agrees with a portion of the OIG recommendation. As noted in the response to OIG Recommendation #2 above, on October 1, 2006 the AMU began conducting a preliminary review of each Form FD-500 submitted. Form FD-500s found to be missing required information, to include annotating the classification level of the laptop computer, are returned to the submitting division for correction. The FBI disagrees with the specific request to ensure that the contents of the lost or stolen laptop computer accompany the Form FD-500.

Certain security risks arise if a policy were to be implemented requiring the contents of the lost or stolen laptop computer accompany the Form FD-500. As an alternative, the Security Division Policy Manual (effective April 3, 2006) defines reportable incidents which would be applicable to the loss or theft of a laptop computer approved for processing classified or sensitive information. The Policy Manual dictates the Security Division be notified in the event the loss or theft of a laptop computer occurs. The Policy Manual provides guidance for information required within the EC. This alternative action, already in place, adequately addresses this aspect of recommendation 3.

4. **Recommendation:** Revise the Form FD-500 to include:

a. whether or not the loss was reported to the Inspection Division for investigation;

b. separate designation for "sensitive" and "classified" categories;

c. tracking of the classification level of NSI contained on a laptop;

d. whether sensitive information contained personally identifying information; and

e. whether the lost or stolen laptop computer was protected with encryption software.

The FBI agrees with the OIG recommendation. An electronic Form FD-500 is being developed which will capture the items set forth in recommendation 4 (a) - (e). This form is set to be available for use by March 31, 2007. One benefit of making the Form FD-500 available only in an electronic format will be that of providing quick reference links to applicable policy and/or procedures. Further, as of January 31, 2007, a mandatory field will appear in Property Management Application requiring the classification level approved for a laptop computer, thus providing an automated tracking mechanism to specifically address Recommendation 4 (c) above.

5. **Recommendation:** Ensure that the Security Division performs a damage assessment of all laptops that are lost or stolen and maintains documentation on this information.

The FBI agrees with the OIG recommendation. Each Division's Chief Security Officer is required to ensure a damage assessment is completed with the results incorporated in the formal notification reporting the loss or theft of a laptop computer.

6. **Recommendation:** Ensure that weapon and laptop losses are appropriately entered into NCIC.

The FBI agrees with the OIG recommendation. As noted in the response to recommendation #4 above, an electronic Form FD-500 is being developed which will capture the items set forth in recommendation 4 (a) - (e). In addition, information already being captured on the Form FD-500, such as NCIC entry data, will be maintained. Also, the initial vetting of the Form FD-500 information for completeness being conducted by AMU since October 1, 2006 will ensure the appropriate NCIC information has been captured.

7. **Recommendation:** Assign to the Asset Management Unit monitoring responsibilities over weapon and laptop losses to ensure that all proper notifications are made.

The FBI agrees with the OIG recommendation. As of January 3, 2007 the AMU assumed the responsibility for ensuring all appropriate FBI entities are made aware of the receipt of Form FD-500s reporting the loss/theft of FBI weapons and laptop computers. AMU will provide copies of the Form FD-500 and any related documentation/information received to components entities for appropriate follow up investigative and/or administrative action.

In addition, a summary EC restating all existing policy related to the response to the loss or theft of a weapon or laptop computer will be prepared and disseminated to all division heads no later than February 15, 2007. Along with this step, AMU will provide, on a monthly basis, to the Assistant Director, Finance Division, copies of all Form FD-500's received reporting losses or thefts of all weapons and laptop computers.

Internal Controls

8. **Recommendation:** Maintain and submit complete, accurate, and timely reports to the DOJ CIO containing all appropriate FBI laptops authorized to process classified information.

The FBI agrees with this recommendation. A review of existing report submission policies is ongoing to determine the appropriate guidance and monitoring needed to ensure all required and applicable reporting is submitted timely to the DOJ, CIO. This review, resulting in additional guidance, will be complete by February 28, 2007.

9. **Recommendation:** Improve the documentation supporting the destruction of excess laptop computers and hard drives.

The FBI agrees with this recommendation. A review of existing policies is ongoing to provide additional guidance supporting the proper completion of all required steps for the disposal of excess laptop computers and hard drives. This review, resulting in additional guidance, will be complete by March 31, 2007.

10. **Recommendation:** Revise its guidance regarding when field offices can degauss their own hard drives.

The FBI agrees with this recommendation. A review of existing policies is ongoing to provide additional guidance relating to the procedures for the degaussing of hard drives. This review, resulting in additional guidance, will be complete by March 31, 2007.

11. **Recommendation:** Submit complete, accurate, and timely Semiannual Reports to the JMD, FASS.

The FBI agrees with this recommendation. A review of existing report submission policies is ongoing to determine the appropriate guidance and monitoring needed to ensure all required and applicable reporting is submitted in a timely manner. This review, resulting in strengthening the existing reporting processes as well as additional guidance, will be complete by February 28, 2007.

12. **Recommendation:** Submit complete, accurate, and timely incident reports summarizing the loss of appropriate FBI laptop computers to the DOJCERT, as required.

The FBI agrees with this recommendation. As noted in earlier responses, a review of existing report submission policies is ongoing to determine the appropriate guidance and monitoring needed to ensure all required and applicable reporting is submitted timely. This review, resulting in additional guidance for reporting to DOJCERT, will be complete by February 28, 2007.

13. **Recommendation:** Strengthen the exit processing for departing employees to ensure that all weapons, laptops, and other issued property is returned to the FBI.

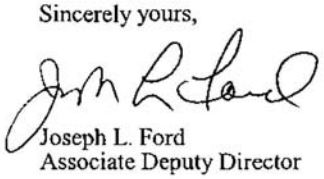
The FBI disagrees with this recommendation. The Report states "Based on our overall review of the 160 weapon losses, we concluded that four of the lost or stolen weapons were the result of an agent leaving the FBI and not returning their weapon. In our judgement, the FBI has not sufficiently strengthened its exit processing for departing employees."

In this case specifically, all four weapons cited as lost due to Agents not returning their property subsequent to separation from the FBI occurred prior to January 31, 2002, the end of the prior audit period. These weapons were, in fact, reported due to the FBI's efforts to strengthen accountability in this particular area of property management and were discovered based on those efforts. The FBI acknowledges the fact that sufficient documentation was not maintained with regard to the 50 separated employees selected for testing during the current audit period but would also point out that none of the weapons or laptop computers reported as lost or stolen during this audit period were linked to anyone in the OIG sample.

As a counter proposal to Recommendation 13, the FBI proposes to issue additional guidance to division heads restating the current policies and procedures to be implemented upon the separation of an employee while also emphasizing the need to maintain proper documentation of such actions. This guidance will be prepared and issued by January 31, 2007.

The FBI has made and continues to make significant improvements and changes to ensure consistent enforcement of existing policies related to the loss and theft of weapons and laptop computers. We appreciate this opportunity to respond to your recommendations and will report to you on a regular basis with regard to our implementation progress.

Sincerely yours,



Joseph L. Ford
Associate Deputy Director

OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

We provided a draft audit report to the FBI for review and comment. The FBI's comments, which detail the actions it has taken or plans to implement in response to our recommendations, have been included as Appendix XVIII to this report.

In its response, before responding to the recommendations, the FBI expressed its disagreement with the inclusion of 43 of the 160 weapons reported as lost or stolen during the 44-month period reviewed in this follow-up audit. The FBI points out that while these 43 weapons were reported as lost or stolen during the current review period, the loss actually occurred prior to this period. We included these 43 weapons in the totals for several reasons. First, our approach in the follow-up audit was consistent with our approach in the original 2002 audit of FBI accountability for weapons and laptops that also included weapons lost or stolen prior to the review period but reported during the review period. Second, none of these 43 weapons were included in the 354 lost or stolen weapons reported in the 2002 audit, so there was no "double counting" in the sample. Third, removing these weapons from the analysis would inaccurately characterize the number of weapons reported by the FBI as lost or stolen during this 44-month period. However, we noted this issue in the report, along with the FBI's objection and the reasons for our methodology.

This Appendix summarizes our analysis of the FBI's comments and proposed actions required to close the report.

Recommendations:

1. **Resolved.** The FBI agreed with our recommendation to ensure that the AMU maintains all Forms FD-500 with accompanying documentation and required information. In response, the FBI stated that the AMU began scanning and electronically maintaining all Forms FD-500 and accompanying documentation and required information. In addition, the FBI stated that all previously submitted and processed Forms FD-500 will be scanned for electronic retention purposes, as resources permit. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented (for example, periodic reconciliations between Forms FD-500 and a PMA list of lost and stolen weapons and laptop

computers) to ensure that the AMU maintains all Forms FD-500.

2. **Resolved.** The FBI agreed with our recommendation to ensure that the most current version of the Form FD-500 is used to report weapon and laptops losses. In its response, the FBI stated that on October 1, 2006, the AMU began conducting preliminary reviews of each submitted Form FD-500 and intends to return any outdated form back to the originating field office for correction and proper submission. This recommendation can be closed when the FBI provides to us a copy of the directive that instructed the AMU to perform preliminary reviews of Forms FD-500.

3. **Resolved.** The FBI agreed with our recommendation to ensure that all Forms FD-500 that are submitted to the AMU are complete, accurate, and timely. In its response, the FBI stated that on October 1, 2006, the AMU began conducting preliminary reviews of each submitted Form FD-500. The FBI said that forms found to be lacking required information are returned to the submitting office for correction.

   However, the FBI stated that it disagreed with our specific request to ensure that a description of the contents of lost or stolen laptop computers accompany the Forms FD-500. The FBI cited security risks as the reason for why the content information should not accompany the Forms FD-500 to the AMU. Also, the FBI stated that it already has policy in place requiring that its Security Division be notified in the event of a laptop loss or theft and that this requirement adequately addresses our recommendation.

   In our report, we stated that "[a]side from reviewing the Forms FD-500 we asked FBI officials if they could determine the content of the 51 lost or stolen laptop computers and whether they contained sensitive or classified information. FBI officials explained that they did not maintain such information and, therefore, could not determine the content of the laptops or whether sensitive or classified information was contained on them. We asked FBI officials why they do not have this information. Security Division officials speculated that the SCU may not have been notified of the lost and stolen laptop computers and, therefore, would not have followed up in determining the contents of the lost or stolen laptops."

   Further, we stated in our report that "FBI officials acknowledged to the OIG that there was a breakdown in obtaining necessary information on the contents of the laptops that were lost or stolen. The FBI Security

officials suggested that part of the cause may be attributed to the lack of a centralized unit within the FBI that could identify the contents of lost or stolen laptops or make sure that Forms FD-500 are complete and accurate." In addition, we noted that some of the Forms FD-500 that we reviewed were accompanied by general descriptions of the contents of the lost or stolen laptops. However, a description of laptop contents was not found for all Forms FD-500 relating to lost and stolen laptops.

Based on these results, our intent was to recommend that not only should the AMU ensure that Forms FD-500 be complete, accurate, and timely, but also that a general description of the contents of lost or stolen laptops be submitted to the Security Division. The specific request in our recommendation would ensure that the Security Division receives adequate information in order for it to be able to appropriately address laptop losses and perform timely damage assessments. We do not believe this would present a security concern, but rather it would be consistent with the FBI's security policy. Therefore, we consider this recommendation to be resolved. To close this recommendation, please provide us with a copy of the directive that instructed the AMU to perform preliminary reviews of Forms FD-500 to ensure completeness, accuracy, and timeliness. Also, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure that the Security Division timely receives a general description of the contents of lost or stolen laptops.

4. **Resolved.** The FBI agreed with our recommendation to revise the Forms FD-500 to include additional information such as whether or not the loss was reported to the Inspection Division for investigation, the classification level of National Security Information contained on the laptop, whether the laptop contained personal identifying information, and whether the laptop was protected with encryption software. The FBI stated that it was developing an electronic Form FD-500 that will capture this information. In addition, the FBI stated that a mandatory field will appear in the PMA requiring the classification level approved for each laptop computer. This recommendation can be closed when we receive evidence that the Form FD-500 was revised and a new field relating to laptop classification levels was added to the PMA.

5. **Resolved.** The FBI agreed with our recommendation to ensure that the Security Division performs a damage assessment of all laptops that are lost or stolen and maintains documentation on this information. The FBI stated that each Division's Chief Security Officer is required to

ensure that damage assessments are completed and the results are incorporated in the formal notification reporting the loss or theft of a laptop computer. This recommendation can be closed when the FBI provides evidence of new or strengthened controls that have been established to ensure that the Division's Chief Security Officers are conducting and properly reporting damage assessments of lost or stolen laptop computers.

6. **Resolved.** The FBI agreed with our recommendation to ensure that weapon and laptop losses are appropriately entered into NCIC. The FBI stated that this recommendation will be addressed with the development of the new electronic Form FD-500 that will capture information related to the NCIC entry and the AMU's preliminary review of the Forms FD-500 information for completeness. This recommendation can be closed when the FBI provides evidence of the revised Form FD-500 and a copy of the directive that instructed the AMU to perform preliminary reviews of Forms FD-500 information to ensure completeness.

7. **Resolved.** The FBI agreed with our recommendation to assign to the AMU monitoring responsibilities over weapon and laptop losses to ensure that all proper notifications are made. The FBI stated that as of January 3, 2007, the AMU assumed the responsibility for ensuring that all appropriate FBI entities are made aware of the receipt of Forms FD-500 reporting the loss or theft of weapons and laptop computers. The AMU will provide copies of Forms FD-500 and related documentation to FBI entities responsible for investigative and administrative follow-up action in weapon and laptop losses. In addition, the FBI stated that it will notify all divisions no later than February 15, 2007, of all existing policy related to the issue of responding to lost or stolen weapons and laptop computers. Further, the AMU will provide, on a monthly basis, copies of all Forms FD-500 received to the Assistant Director, Finance Division. This recommendation can be closed when we receive a copy of the directive that assigned monitoring responsibilities to the AMU to ensure proper notifications are made regarding lost or stolen weapons and laptops. In addition, please provide a copy of the summary electronic communication that will be disseminated to all FBI divisions no later than February 15, 2007, regarding all existing policy on responding to lost or stolen weapons and laptops.

8. **Resolved.** The FBI agreed with our recommendation to maintain and submit complete, accurate, and timely reports to the DOJ CIO containing all appropriate FBI laptops authorized to process classified

information. The FBI stated that it was reviewing existing report submission policies to determine the appropriate guidance and monitoring needed to ensure all required and applicable reporting is submitted timely to the DOJ CIO. This review will be completed by February 28, 2007. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure the FBI provides complete, accurate, and timely reports to the DOJ CIO.

9. **Resolved.** The FBI agreed with our recommendation to improve the documentation supporting the destruction of excess laptop computers and hard drives. The FBI stated that it was reviewing existing policies in order to provide additional guidance that will support the proper completion of all required steps related to the disposal of excess laptop computers and hard drives. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure the FBI maintains supporting documentation related to the destruction of excess laptop computers and hard drives.

10. **Resolved.** The FBI agreed with our recommendation to revise its guidance regarding when field offices can degauss their own hard drives. The FBI stated that it was reviewing existing policies in order to provide additional guidance on procedures for the degaussing of hard drives. To close this recommendation, please provide a copy of any guidance developed regarding when field offices can degauss their own hard drives.

11. **Resolved.** The FBI agreed with our recommendation to submit complete, accurate, and timely semiannual reports summarizing the loss and theft of property to the JMD. The FBI stated that it was reviewing existing report submission policies to determine the appropriate guidance and monitoring needed to ensure all required and applicable reporting is submitted in a timely manner. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure the FBI submits complete, accurate, and timely semiannual reports to JMD.

12. **Resolved.** The FBI agreed with our recommendation to submit complete, accurate, and timely incident reports summarizing the loss of appropriate FBI laptop computers to the DOJCERT, as required. The FBI stated that it was reviewing existing report submission policies to determine the appropriate guidance and monitoring needed to ensure

all required and applicable reporting is submitted timely. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure the FBI submits complete, accurate, and timely reports to DOJCERT.

13. **Resolved.** The FBI stated that it disagreed with this recommendation, but it proposed action that satisfies the intent of our recommendation. It acknowledged that sufficient documentation was not maintained with regard to the 50 separated employees selected for testing during the current audit period. The FBI proposed to issue additional guidance by January 31, 2007, to division heads restating the current policies and procedures to be implemented upon the separation of an employee and emphasizing the need to maintain proper documentation of such actions. These proposed actions would strengthen exit processing for departing employees, which addresses the intent of our recommendation. To close this recommendation, please provide evidence of new or strengthened controls and additional guidance that have been implemented to ensure the FBI maintains proper documentation on its exit processing of departing employees.