

# **THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES' CONTROLS OVER ITS WEAPONS, LAPTOP COMPUTERS, AND OTHER SENSITIVE PROPERTY**

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

Audit Report 08-29  
September 2008

**This page left blank intentionally.**

# **THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES' CONTROLS OVER ITS WEAPONS, LAPTOP COMPUTERS, AND OTHER SENSITIVE PROPERTY**

## **EXECUTIVE SUMMARY**

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) employs 4,845 Special Agents, Explosives Industry Operations Investigators, and support personnel. To fulfill the ATF's mission, these personnel are responsible for maintaining the agency's weapons, laptop computers, and other sensitive property such as ammunition and explosives. As of August 17, 2007, ATF had 22,476 weapons and 7,505 laptop computers assigned to ATF offices and employees located throughout the United States and in 5 foreign countries.

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 DOJ's accountability for such property. The OIG performed a series of audits during fiscal year (FY) 2002 that examined controls over weapons and laptop computers at the Federal Bureau of Investigation (FBI), Federal Bureau of Prisons, Drug Enforcement Administration (DEA), and United States Marshals Service.<sup>1</sup> We found substantial losses and weak controls over management of this property throughout DOJ law enforcement agencies.

ATF transferred to DOJ in January 2003 from the Department of the Treasury (Treasury) after the OIG completed its first round of weapons and laptop audits.<sup>2</sup> In 2002, the Treasury OIG had conducted an audit of ATF's controls over sensitive property, including firearms, laptop computers, ammunition, and explosives.<sup>3</sup> The Treasury audit concluded that ATF's

---

<sup>1</sup> U.S. Department of Justice, Office of the Inspector General, *The Department of Justice's Control Over Weapons and Laptop Computers Summary Report*, Audit Report 02-31, (August 2002).

<sup>2</sup> ATF's law enforcement functions became part of the Department of Justice on January 24, 2003, as a result of the Homeland Security Act.

<sup>3</sup> U.S. Department of the Treasury, Office of Inspector General, *Protecting the Public: Bureau of Alcohol, Tobacco and Firearms' Control over Sensitive Property Is Adequate*, Audit Report 02-097, (June 2002).

controls over firearms and laptop computers were adequate and that ATF generally took appropriate actions in response to lost, stolen, or missing property. The audit also concluded that ATF's controls over ammunition and explosives needed improvement. ATF concurred with the findings and recommendations in the review and subsequently reported that it had implemented new controls to address these weaknesses.

As a result of Treasury's 2002 audit, ATF required all its divisions to conduct a baseline inventory of ammunition and report the results to headquarters. ATF required that an annual 100-percent inventory of all ATF-owned ammunition be performed and that such reviews include a disinterested person to assist in conducting ammunition inventories.<sup>4</sup> ATF also required that a disinterested person directly participate in all future inventories of ATF explosives. In addition, ATF required that records of each type of ATF-owned ammunition and explosive be maintained indefinitely.

### **OIG Audit Approach**

This audit of the ATF's controls over its weapons, laptop computers, and other sensitive property is one of a series of follow-up audits that the OIG is conducting to examine DOJ components' controls over their weapons and laptop computers.<sup>5</sup> The objectives of this audit were to assess: (1) the adequacy of ATF's actions taken in response to weapons, laptop computers, ammunition, and explosives identified as lost, stolen, or missing; and (2) the effectiveness of ATF's internal controls over weapons, laptop computers, ammunition, and explosives. Our other audits of controls over weapons and laptop computers in DOJ components did not include a review of ammunition and explosives. However, we included ammunition and explosives in this audit because the 2002 Treasury OIG audit identified weaknesses in these areas. Our review covered the 59-month period from October 1, 2002, through August 31, 2007.

---

<sup>4</sup> The ATF policy does not define "disinterested person." The Treasury audit report defined the term as a person who is independent of daily responsibility for the inventory and independent of the custodial function. In this report, we have used ATF's terminology when citing the requirement.

<sup>5</sup> See, e.g., U.S. Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Control Over Weapons and Laptop Computers Follow-Up Audit*, Audit Report 07-18, (February 2007) and U.S. Department of Justice, Office of the Inspector General, *The Drug Enforcement Administration's Control Over Weapons and Laptop Computers Follow-Up Audit*, Audit Report 08-21, (March 2008).

During this audit, we interviewed or met with various ATF officials, including ATF's Chief Financial Officer and Chief of the Materiel Management Branch.<sup>6</sup> We also reviewed documents and tested controls at ATF headquarters offices in Washington, D.C.; Landover, Maryland; Martinsburg, West Virginia; 7 field divisions and 24 field offices associated with those divisions; and 3 ATF training facilities.

Our audit examined ATF's actions in response to lost, stolen, or missing weapons, laptop computers, ammunition, and explosives, and whether ATF followed current DOJ procedures after weapons or laptop computers were lost, stolen, or missing. We also queried the National Crime Information Center (NCIC) to identify lost, stolen, or missing ATF weapons and laptop computers that were recovered or weapons used in the commission of a crime. We also examined whether national security or investigative information may have been contained on ATF lost laptop computers.

In addition, we reviewed ATF's internal controls over accountable property, its exit procedures for departing employees, and its disposal of property. Our review included a physical verification of a sample of weapons and laptop computers. We also tested the accuracy and completeness of the property records, and we reviewed controls over ammunition and explosives to determine whether ATF stores and properly accounts for this property. Appendix I contains a further description of our audit objectives, scope, and methodology.

## **OIG Results in Brief**

Over the 59-month period we tested, 76 weapons and 418 laptop computers were lost, stolen, or missing from ATF. ATF's rate of weapons loss per month has nearly tripled since Treasury's 2002 audit, and the rate of loss per month for laptop computers was 50 times higher than what the 2002 audit revealed. According to ATF officials, the much higher rate of laptop computer losses resulted primarily from adjustments ATF made to its inventory records to correct inaccurate data accumulated over several years.

We also found serious deficiencies in ATF's response to these lost, stolen, or missing items. ATF staff did not report many of the lost, stolen, or missing weapons and laptop computers to ATF's Internal Affairs Division (Internal Affairs), as required by ATF's property management policies. In

---

<sup>6</sup> "Materiel" is a term used to refer to equipment and supplies, especially in military organizations, which is also used by ATF.

addition, ATF did not report most of the missing laptop computers to ATF Internal Affairs for investigation. We also found that ATF staff did not enter 5 lost, stolen, or missing weapons into NCIC and did not document what data was contained on 398 of the 418 lost, stolen, or missing laptop computers. Consequently, ATF could not provide assurance that these computers did not contain sensitive information, personally identifiable information (PII), or classified information. Because ATF did not begin to install encryption software on its laptop computers until May 2007, few if any of the laptop computers lost, stolen, or missing during our review period were protected.<sup>7</sup>

Treasury's 2002 audit reported that ATF's controls over firearms and laptop computers were adequate. However, our audit identified weaknesses in several areas. First, ATF staff could not locate several active weapons and several laptop computers sampled for our review. Second, ATF staff did not maintain accurate and complete records in ATF's property management system, nor was the system regularly updated as required by ATF's property management policy. In addition, ATF did not maintain adequate documentation for disposed weapons and laptop computers and did not ensure that it had cleared computer hard drives prior to disposal.

ATF, like all DOJ components, is also required to report to DOJ information regarding losses of weapons and laptop computers. However, ATF staff did not report any lost, stolen, or missing weapons and laptop computers in the required semiannual reports to DOJ. ATF staff also did not report to DOJ the number of laptop computers authorized to process National Security Information (NSI), and ATF did not report 16 incidents of lost laptop computers to the DOJ's Computer Emergency Response Team (DOJCERT), as required by Department policy.

Our audit concluded that ATF had adequate controls over the explosives in its possession. We also concluded that ATF had proper physical security over its ammunition. However, we identified continued weaknesses in ATF's ammunition accountability and controls. We tested accountability and controls for ammunition at 20 ATF field offices during our audit and found that 11 field offices followed perpetual inventory recordkeeping requirements for ammunition, but 9 offices did not maintain

---

<sup>7</sup> Encryption software protects information on computers so that the information is unreadable without proper authorization.

such records.<sup>8</sup> Also, ATF could not provide documentation that any field office had submitted annual ammunition inventories to ATF headquarters, as required by ATF policies.

In our report, we make 14 recommendations to assist ATF in improving its controls over weapons, laptop computers, and ammunition.

Our report contains detailed information on the full results of our review of ATF's control over weapons, laptop computers, ammunition, and explosives. The remaining sections of this Executive Summary describe in more detail our audit findings.

### **ATF'S Weapon, Laptop Computers, Ammunition, and Explosives Losses**

To determine the number of lost, stolen, or missing weapons and laptop computers, we reviewed records maintained by ATF's Internal Affairs and property management office. We also reviewed incident reports of lost, missing, or stolen property reported to Internal Affairs and the results of any subsequent investigations, including any disciplinary actions that were taken. We also assessed the results of periodic inventories that field offices submitted to ATF headquarters, and the documents the property management office used to remove weapons and laptop computers from the property records. Inventory results included lists of property that field offices reported as missing during periodic inventories. We also interviewed field staff to obtain information about ammunition and explosives losses.

#### *Rates of Weapon and Laptop Computer Losses*

For perspective on ATF's 76 weapons and 418 laptop computers identified as lost, stolen, or missing, we developed loss rates to compare both with the loss rates previously reported for ATF and with those experienced by other DOJ components. We were able to identify comparable information in the 2002 Treasury audit report and in OIG audit reports for the FBI and DEA.

To compare losses during our 59-month audit period with Treasury's 2002 audit findings, we used the measure "losses per month" because the audit periods were different lengths. We determined that ATF's rates of loss

---

<sup>8</sup> Perpetual inventory is an inventory accounting system in which book inventory is updated continuously, as opposed to periodic inventories in which updates are made on a recurring basis.

for both weapons and laptop computers had significantly increased since the 2002 Treasury audit report.

The following table shows the total losses per month for weapons and laptop computers for both audits. We used the Reports of Survey and the Internal Affairs investigative reports to categorize the items summarized in the table. The two right columns compare the losses per month between our audit period and the period covered by the 2002 Treasury audit. The 1.29 weapons lost per month for our audit period was nearly three times the 0.47 weapons lost per month reported by the Treasury in 2002. The 7.08 laptop computers losses per month for our audit period were approximately 50 times the 0.14 computer losses per month reported by Treasury OIG.



**LOST, STOLEN, OR MISSING WEAPONS AND LAPTOP COMPUTERS**

<b>Category</b>	<b>Number of lost, stolen, or missing Items Reported</b>		<b>Losses Reported Per Month</b>	
	<b>2002 Audit (36-month period)</b>	<b>Current Audit (59-month period)</b>	<b>2002 Audit</b>	<b>Current Audit</b>
Lost weapons	4	19	0.11	0.32
Stolen weapons	13	35	0.36	0.59
Weapons determined missing during an inventory	0	12	0.00	0.20
Weapons which could not be categorized as lost, stolen, or missing because documents had been destroyed or were missing <sup>9</sup>	0	10	0.00	0.17
<b>Lost, Stolen, or Missing Weapons</b>	<b>17</b>	<b>76</b>	<b>0.47</b>	<b>1.29<sup>10</sup></b>
Lost laptop computers	0	8	0.00	0.14
Stolen laptop computers	0	50	0.00	0.85
Laptop computers determined missing during an inventory	0	274	0.00	4.64
Laptop computers which could not be categorized as lost, stolen, or missing because documents had been destroyed or were missing <sup>9</sup>	5	86	0.14	1.46
<b>Lost, Stolen, or Missing Laptop computers</b>	<b>5</b>	<b>418</b>	<b>0.14</b>	<b>7.08<sup>11</sup></b>

Source: OIG analysis of ATF data

<sup>9</sup> ATF staff told us the records for 8 of the 10 weapons and for 78 of the 86 laptop computers were destroyed in accordance with ATF's written policy that personal property records are to be destroyed 3 years after the property is disposed of. ATF staff could not locate the other records.

<sup>10</sup> The column does not add up to 1.29 due to rounding.

<sup>11</sup> The column does not add up to 7.08 due to rounding.

All of the items included in the table were reported within ATF as lost, stolen, or missing during a periodic physical inventory conducted by ATF staff.<sup>12</sup> Lost and stolen weapons and laptop computers are discussed later in this executive summary. When items are identified as missing, either during an inventory or otherwise, ATF staff must prepare "Reports of Survey" to explain the losses.

Some but not all of the lost, stolen, or missing items were reported to ATF Internal Affairs, which prepared investigative reports regarding the circumstance of the loss. Of the 76 lost, stolen, or missing weapons, 63 were reported to Internal Affairs. Of the 418 lost, stolen, or missing laptop computers, 53 were reported to Internal Affairs.<sup>13</sup>

The table shows that 12 weapons were identified as missing during a physical inventory. The 12 missing weapons represent approximately 16 percent of the total lost, stolen, and missing weapons. Investigative reports at Internal Affairs indicated that 6 of the missing weapons were later recovered.

We compared ATF's missing weapons with those identified as missing during our prior audits of the DEA and FBI. At the DEA, 4 (4 percent) of 91 lost, missing, or stolen weapons were identified as missing during an inventory. At the FBI, 23 (14 percent) of 160 lost, missing, or stolen weapons were identified as missing during an inventory. ATF's percentage of weapons missing during an inventory (16 percent) is higher than the DEA's percentage and about the same as the FBI's percentage.

The table shows that 274 ATF laptop computers were identified as missing during periodic inventories. These losses represent approximately 66 percent of all lost, stolen, or missing ATF computers. The inventory documentation submitted to ATF headquarters provided a variety of reasons for the missing computers. The primary reason was that managers believed the computers were returned to the supplier, exchanged for newer models, or donated to schools after becoming obsolete. However, managers could not demonstrate this had occurred because they could not produce the

---

<sup>12</sup> There is no overlap between items between the categories.

<sup>13</sup> Laptop computers identified as missing during an inventory were generally not reported to Internal Affairs. We could not determine the circumstances for weapons not being reported because ATF could not provide documentation about 10 of the 13 weapons not reported to Internal Affairs. The other three were reported missing on Reports of Survey and were treated as inventory adjustments.

required documentation for such returns, exchanges, or donations. Consequently, we include these items in our analysis as missing, which is how we treated this issue in our DEA and FBI audits.

We also compared the percentage of ATF's missing laptop computers with those identified as missing during our prior audits of the DEA and FBI. At the DEA, 149 (65 percent) of 231 lost, stolen, or missing laptop computers were identified as missing during an inventory. At the FBI, 62 (39 percent) of 160 lost, stolen, or missing laptop computers were missing during an inventory. ATF's percentage of laptop computers missing during an inventory (66 percent) is nearly equal to the percent missing at the DEA and higher than the percent missing at the FBI.

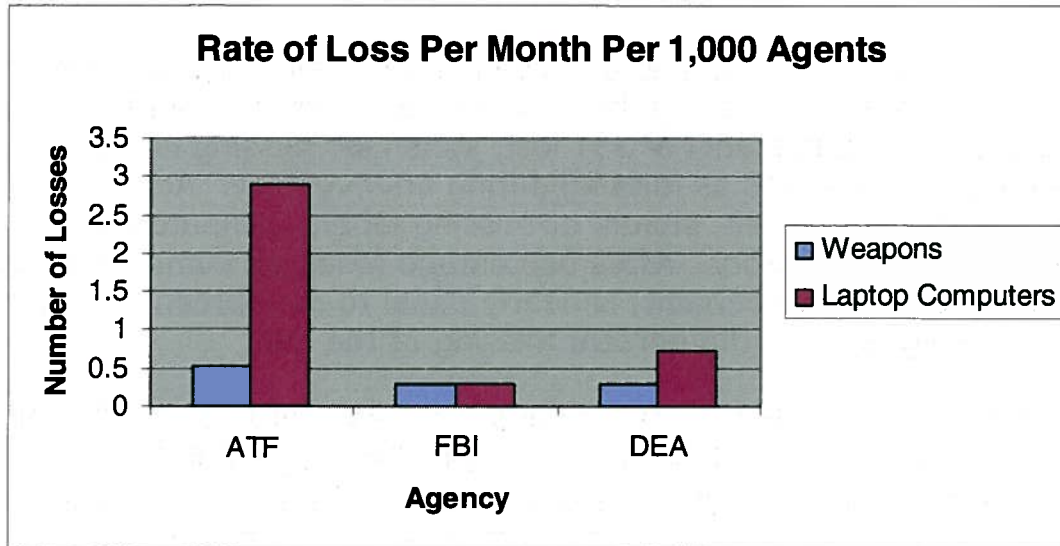
For 10 of the 76 lost, stolen, or missing weapons and for 86 of the 418 lost, stolen or missing laptop computers, the Reports of Survey had been destroyed at the end of the required record-retention period or were otherwise missing and no investigation reports were prepared.<sup>14</sup> Consequently, we could not determine how these losses should be categorized – lost, stolen, or missing.

To compare ATF's losses with those reported in audits of weapons and laptop computers at the FBI and DEA, we also calculated rates of loss per 1,000 agents because the components vary widely in number of employees. As the following table shows, for our 59-month audit period, ATF's rate for lost, stolen, or missing weapons (0.52) was nearly double those of the FBI (0.29) and DEA (0.28). ATF's losses of laptop computers were significantly higher at nearly 3 per 1,000 agents, compared with less than 1 per 1,000 FBI or DEA agents. The following chart shows the loss rates reported in audit reports for these three DOJ components.

---

<sup>14</sup> We know from the property management system that these items were removed based on Reports of Survey. ATF staff told us the records for 8 of the 10 weapons and for 78 of the 86 laptop computers were destroyed in accordance with ATF's written policy that personal property records are to be destroyed 3 years after the property is disposed of. ATF staff could not locate the other records. Later in this Executive Summary and in Finding I, we discuss concerns regarding reporting items to Internal Affairs.

**ATF, FBI, AND DEA LOST, STOLEN, OR MISSING  
WEAPONS AND LAPTOP COMPUTERS**



Source: OIG analysis of ATF, FBI, and DEA data

*Types of Losses*

We found that 35 (46 percent) of the ATF's 76 weapons lost, stolen, or missing during this review period were stolen from Special Agents' residences, hotel rooms, and government-owned or privately-owned vehicles. The remaining 41 (54 percent) of the 76 lost, stolen, or missing weapons were identified as missing during an inventory, left in a public place, lost during shipping, lost under other circumstances, or the losses were unexplained. We determined that in 40 of the 76 losses (53 percent), the loss or theft of weapons appeared to have resulted from employees' carelessness or failure to follow ATF policy.

For laptop computers, we found that 50 (12 percent) of the 418 were stolen. Of these, 21 were stolen from a vehicle; 20 were stolen from an office, residence, or hotel; and 9 were unexplained because ATF could not provide information on the nature of the theft. Of the remaining 368 lost, stolen, or missing laptop computers, 274 were identified as missing during an inventory and 94 were lost during shipping, left in a public place, or were unexplainably lost.

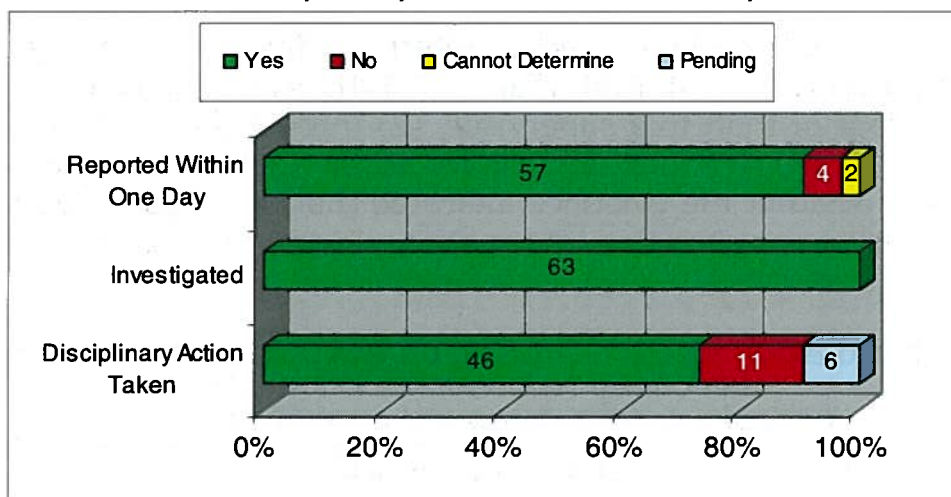
*Reporting Weapons Losses*

All lost, stolen, or missing weapons are required by ATF Order 1850.2C to be reported to ATF Internal Affairs. Of the 76 lost, stolen, or missing

weapons, ATF reported 63 (83 percent) to Internal Affairs. As of July 2008, ATF was unable to explain to us why the remaining 13 weapons (17 percent) were not reported.

For the 63 weapons losses that were referred to Internal Affairs, we reviewed documentation to determine whether: (1) the employee immediately reported the loss or theft to a supervisor; (2) Internal Affairs investigated the incident; and (3) ATF took disciplinary action against the employee, if appropriate.<sup>15</sup> We summarize the results in the following chart.

**ACTIONS TAKEN ON 63 LOST, STOLEN, OR MISSING WEAPONS  
REPORTED TO INTERNAL AFFAIRS<sup>16</sup>  
OCTOBER 1, 2002, THROUGH AUGUST 31, 2007**



Source: OIG analysis of ATF data

We found that ATF investigated all lost, stolen, or missing weapons reported to Internal Affairs and appeared to take appropriate disciplinary action in these cases. Two weapons ATF staff reported as stolen were used to commit crimes. One weapon, stolen from an ATF vehicle parked at the Special Agent's residence, was recovered after a suspect used the stolen weapon to shoot through the window of a residence. Another weapon, stolen from an ATF Special Agent's residence, was recovered from suspects arrested in connection with a burglary.

<sup>15</sup> ATF policy requires that lost, stolen, or missing weapons and laptop computers be reported to a supervisor "immediately." ATF did not further define what was meant by immediately. We considered a loss to have been reported "immediately" if it was reported within 1 day.

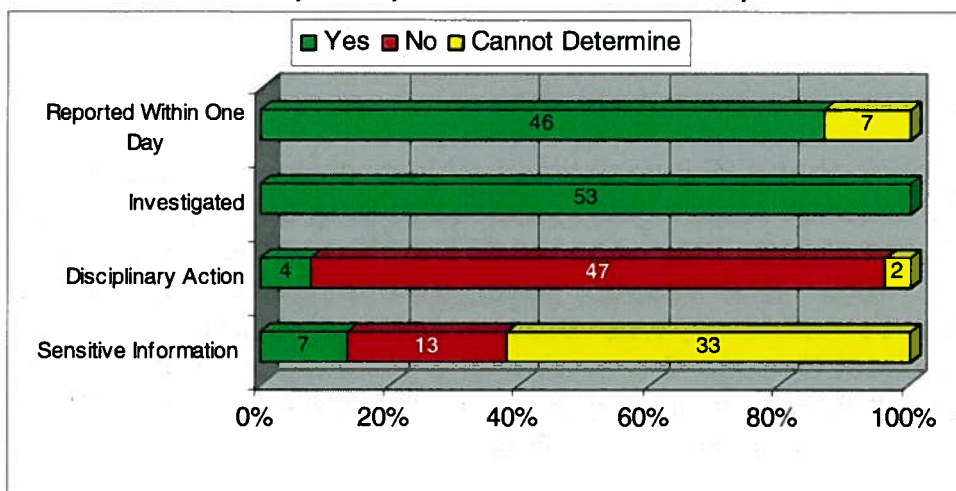
<sup>16</sup> For a comprehensive list of lost, stolen, or missing weapons, see Appendix III.

## Reporting Laptop Computer Losses

ATF policy requires that all lost, stolen, or missing laptop computers be reported to Internal Affairs. Of the 418 laptop computers identified as lost, stolen, or missing during the 59-month audit period, 274 (66 percent) were reported as not being located during a physical inventory. ATF officials told us that they do not report inventory discrepancies as missing property to Internal Affairs. That policy is also consistent with DOJ policy.<sup>17</sup> However, of the remaining 144 laptop computers, ATF only reported 53 (37 percent) to Internal Affairs. We concluded that ATF did not follow proper procedures to report the remaining 91 laptop computer losses and did not provide a reason why it did not report those losses.

From information maintained by Internal Affairs, we examined whether in the cases reported to Internal Affairs: (1) the ATF employee immediately reported the loss or theft to a supervisor, (2) Internal Affairs investigated the incident, and (3) ATF took disciplinary action against the employee. We also reviewed whether the evidence indicated that the missing laptop contained sensitive or classified information. We summarize the results in the following chart.

**ACTIONS TAKEN ON 53 LOST, STOLEN, OR MISSING LAPTOP COMPUTERS REPORTED TO INTERNAL AFFAIRS<sup>18</sup>**  
**OCTOBER 1, 2002, THROUGH AUGUST 31, 2007**



Source: OIG analysis of ATF data

<sup>17</sup> DOJ policy refers to reporting losses to a Board of Survey. DOJ does not require apparent inventory processing discrepancies to be referred to a Board of Survey.

<sup>18</sup> For a comprehensive list of lost, stolen, or missing laptop computers, see Appendix IV.

We found that ATF investigated all lost, stolen, or missing laptop computers reported to Internal Affairs, although few of those investigations resulted in disciplinary actions against the employees responsible for the losses.

### *Contents of Lost, Stolen, or Missing Laptop Computers*

ATF's property management policy does not include written procedures requiring ATF to assess the contents of lost, stolen, or missing laptop computers. As explained below, we found that ATF did not regularly attempt to determine whether the lost, stolen, or missing laptop computers contained sensitive or classified information.

ATF's Information Systems Security Officer from the Office of Science and Technology (OST) told us that staff from OST and Internal Affairs interview users about the content of lost, stolen, or missing laptop computers when staff report them missing. OST staff also told us the results of those interviews are documented in ATF Internal Affairs reports and incident reports submitted to DOJCERT.

We asked ATF for incident reports submitted to DOJCERT and ATF Internal Affairs reports on all 53 lost, stolen, or missing laptop computers reported to Internal Affairs. We did not ask for more than these 53 because we knew ATF did not have any records for the others.

ATF provided all 53 Internal Affairs reports. However, it provided DOJCERT reports for only 6 (11 percent) of the 53 laptop computers.<sup>19</sup> Those reports indicated that ATF made inquiries into the contents of 20 lost, stolen, or missing laptop computers. Seven of the reports indicated that the lost laptop computers contained sensitive information, and 13 reports indicated that the lost laptop computers did not contain either sensitive or classified information.

ATF could not provide adequate information regarding whether the remaining 398 lost, stolen, or missing laptop computers contained sensitive or classified information. Without knowing the contents of lost, stolen, or missing laptop computers, ATF could not assess what damage these losses could have had on ATF's operations or national security. Moreover, since

---

<sup>19</sup> ATF provided DOJCERT reports for nine other lost, stolen, or missing laptop computers. Four were lost, stolen, or missing during the period covered by our audit and five were lost, stolen, or missing after the period covered by our audit.

ATF did not begin installing encryption software until May 2007, few if any of these lost, stolen, or missing laptop computers were encrypted.

### *Entering Losses of Weapons and Laptop Computers into NCIC*

ATF policy requires that all lost, stolen, or missing weapons be entered into NCIC. It does not require that lost, stolen, or missing laptop computers be entered into NCIC.<sup>20</sup>

To test how often ATF's lost, stolen, or missing weapons were entered into NCIC, we reviewed documentation during our audit for 72 of the 76 weapons.<sup>21</sup> We found that seven lost, stolen, or missing weapons were not required to be entered into NCIC because the weapons were recovered shortly after being lost or stolen. Of the remaining 65 lost, stolen, or missing weapons, 5 were not entered into NCIC in accordance with ATF's written policy. As of July 2008, ATF staff had not responded to our inquiry about why these losses were not entered into NCIC.

### *Ammunition and Explosives Losses*

ATF has a policy for reporting the loss of explosives, but did not have a specific written policy for reporting the loss of ammunition at the time of our audit. ATF's property management policy requires employees to report losses of government property assigned to them. An ATF official told us that policy covers losses of ammunition, which was specifically included in a revision issued in April 2008. However, the policy in place at the time our audit did not specifically include ammunition and stated that a record is established within the property management system for each property asset, and ammunition is not included in the system. Therefore, it appears that ammunition was property not covered by the property management policy during our audit period. An ATF Internal Affairs manager told us that individual circumstances, such as whether the ammunition was stolen in conjunction with a stolen weapon, dictate whether lost, stolen, or missing ammunition should be referred to Internal Affairs and whether Internal Affairs conducts a full internal investigation into the loss. Because expendable items such as ammunition and explosives are not included in

---

<sup>20</sup> We found that while DOJ policy does not require that lost, stolen, or missing laptop computers be entered into NCIC, the FBI and DEA both have policies that require that lost, stolen, or missing laptop computers be entered into NCIC.

<sup>21</sup> We were unable to test whether four lost, stolen, or missing weapons were entered into NCIC.



ATF's property management system, we could only identify losses that ATF staff reported to Internal Affairs.

### Ammunition

ATF staff reported to Internal Affairs 12 instances of lost, stolen, or missing ammunition for the 59-month period from October 1, 2002, through August 31, 2007. Of the 12 incidents, 1 resulted in an employee receiving a Memorandum of Clearance and another resulted in the employee receiving discipline.<sup>22</sup> There was no full report of investigation for the remaining 10 incidents because a preliminary investigation found no employee misconduct.

### Explosives

ATF reported two instances of lost, stolen, or missing explosives to Internal Affairs during our review period. ATF opened preliminary investigations on both instances, but found no misconduct. The explosives were recovered in both incidents.

## **Internal Controls Over Weapons and Laptop Computers**

DOJ Property Management Regulations require all DOJ components to conduct a physical inventory of all non-expendable personal property, which includes weapons and laptop computers, at least biennially. We determined that ATF had performed annual inventories of weapons and biennial inventories of laptop computers recorded in its automated property system.

We reviewed the ATF inventory reports for the two most recent fiscal years. The reports identified adjustments to the property records based on the physical inventories that were performed. ATF policy requires that shortages of property be reconciled, administrative changes be posted, and that a Report of Survey be prepared for items that could not be reconciled. However, we found that changes were not posted in the ATF's property management system based on inventory reports. As a result, ATF kept many items on the active property list even though it no longer had the property.

---

<sup>22</sup> A Memorandum of Clearance clears the employee of any wrongdoing. This disciplinary action was the result of an investigation that also included review of a weapon loss.

### *Reconciling Property Records to the Financial System*

ATF's financial system is not integrated with its property management system and the two systems are not regularly reconciled. We therefore performed tests to determine whether weapons and laptop computer purchases recorded in ATF's financial system were also recorded in its property management system.

We judgmentally selected from the financial system 4 purchases for 1,264 weapons valued at \$737,133. We traced all the purchases to ensure that the items were entered into the property management system, and we found no discrepancies.

ATF had no laptop computer procurement records to test because its laptop computers are leased rather than purchased outright and entered into the financial system. ATF replaces laptop computers after 3 years with new leased computers, and ATF retains ownership of the laptop computers that are replaced.<sup>23</sup> The ATF disposed of most of the replaced laptop computers, but ATF keeps a few of the replaced computers for special purposes. As a result, all ATF-owned laptop computers at the time of our audit were items that ATF had kept after their leases expired. Therefore, we were unable to determine the adequacy of ATF's controls for reconciling laptop computer property records to the financial system because the leased computers are not entered into the financial system.

### *Accuracy and Completeness of Property Records in the Property Management System*

ATF's property management system accounts for weapons and laptop computers, but we found that it was unable to account for all items located in the system. To evaluate the property management system, we tested weapons and laptop computers in two phases. First, we completed a 100-percent inventory of weapons and laptop computers at ATF's Atlanta and Washington Field Divisions. We then performed a second phase of testing during which we selected from the property management system a statistical sample of weapons and laptop computers located at 14 field

---

<sup>23</sup> This refresh cycle of 3 years is normal in the information technology industry. The monthly lease amount per computer was \$310, which includes \$77 for the laptop and \$233 for support services such as managing the server and providing data security and round-the-clock technical support. Because ATF leased laptop computers and was billed monthly, ATF had no laptop computer purchasing records to test.

offices. We sought to verify the existence of all sampled weapons and laptop computers at the 16 locations tested.

We were able to verify all but 4 (less than 1 percent) of the 1,788 weapons in our sample, and all but 23 (2.2 percent) of the 1,032 laptop computers.

The following table summarizes the results of verification testing at each selected location. Items identified in the table as "Accounted For" are those that we were able to verify through either physical observation by auditors or confirmation memoranda from ATF officials verifying that they had viewed the equipment and confirmed the identifying information, such as manufacturer, model, and serial number or documentation showing that the item had been disposed of.

**SAMPLE TESTING OF WEAPONS AND LAPTOP COMPUTERS  
RECORDED IN THE ATF PROPERTY MANAGEMENT SYSTEM**

Location	WEAPONS		LAPTOP COMPUTERS	
	Accounted For	Unaccounted For	Accounted For	Unaccounted For
Atlanta Field Div. (FD)	331	0	237	1
Washington FD	519	3	229	5
<b>SUBTOTALS</b>	<b>850</b>	<b>3</b>	<b>466</b>	<b>6</b>
Headquarters				
Glynco, GA	92	0	67	2
Landover, MD	0	0	31	0
Martinsburg, WV	165	0	58	0
Kansas City FD				
Kansas City, MO	58	0	53	0
St. Louis, MO	84	0	30	2
Los Angeles FD				
Los Angeles, CA	96	1	49	12
Riverside, CA	31	0	16	0
New Orleans FD				
Little Rock, AR	36	0	21	0
Metairie, LA	59	0	36	1
Shreveport, LA	46	0	18	0
Philadelphia FD				
Philadelphia, PA	77	0	48	0
Pittsburgh, PA	66	0	35	0
San Francisco FD				
San Francisco, CA	64	0	56	0
Las Vegas, NV	60	0	25	0
<b>SUBTOTALS</b>	<b>934</b>	<b>1</b>	<b>543</b>	<b>17</b>
<b>TOTALS</b>	<b>1784</b>	<b>4</b>	<b>1009</b>	<b>23</b>

Source: OIG verification and analysis of ATF property management system data

When we verified all weapons and laptop computers in the Atlanta and Washington Field Divisions, we also determined for each item whether the user and location of the property were accurately recorded in the property management system. Of the 1,316 items we verified in the Atlanta and Washington Field Divisions, we found that 217 (16 percent) had an incorrect user, incorrect location, or both in the property management system record, or the item was not included in the property management system at all.

We also tested the completeness of the property records by tracing weapons and laptop computers in the actual possession of a sample of field office staff back to the property records. For this analysis we selected a

sample of 33 staff at 7 field offices.<sup>24</sup> These 33 staff members maintained 44 weapons and 33 laptop computers in their possession. We traced each item to the property management system to determine if its records were correct. We found that the records for two weapons and four laptop computers reflected incorrect information on users or locations.

During our testing, we also identified items for which conflicting information was entered in the property records. For instance, the property management system database contains data elements to record the office to which the item is assigned and the specific location where it can be found, because some offices operate in multiple locations. We found property records that contained conflicting office and location information, in effect showing the item was in different locations at the same time.

### *Encryption*

ATF began installing encryption software on its laptop computers in May 2007, and ATF staff told us that as of April 2008 ATF had completed the installation on all of its networked laptop computers. The majority of ATF laptop computers are networked and assigned to individuals as personal property.

During our review of accountable property, which occurred from August 2007 through December 2007 and prior to ATF's reported completion of encryption installation, we tested to determine if ATF had installed encryption software on sampled laptop computers. Of the 1,065 laptop computers tested, 63 were unencrypted. Of the 63 unencrypted laptop computers, 42 were used for a dedicated purpose, such as Global Positioning System tracking and video surveillance. ATF personnel told us they do not store sensitive information on these laptop computers. However, the remaining 21 unencrypted laptop computers were assigned to users, such as Special Agents who may have processed sensitive information.

We were unable to test the encryption status of 441 laptop computers because they were verified by confirmation memorandum (180), were unaccounted for (23), or the user was not available to access the encryption software (238).

---

<sup>24</sup> We performed this test at 7 of the 14 field offices (excluding Atlanta and Washington) because all of the personnel at the other 7 locations were already included in another sample we used to trace items from the property records to the person.

DOJ regulations have required that all classified information on a laptop or standalone computer be encrypted. We reviewed the encryption status for ATF's classified laptop computers and found that 5 of the 18 classified laptop computers we tested were not encrypted. By not encrypting classified laptop computers, ATF did not comply with DOJ policy and risked compromising classified information. As of April 2008, ATF reported that it was in the process of encrypting the five unencrypted classified laptop computers.

### *Reporting Requirements for Laptop Computers Containing Classified Information*

Since March 2004, the DOJ Chief Information Officer (CIO) has required all DOJ components, including ATF, to report annually the number of laptop computers it has authorized for processing classified information. However, the DOJ CIO only received a submission from ATF in 2007, and none for any prior years. An ATF official told us that ATF may not have known about the requirement to report classified laptop computers to DOJ.

ATF's 2007 submission included 13 classified laptop computers. However, during our audit we found that ATF had 18 classified laptop computers. The additional five laptop computers were the same five described above as being unencrypted.

### *Reporting Property Losses to DOJ*

DOJ requires all components, including ATF, to submit semiannual reports summarizing thefts of government property during the preceding 6 months. In the 5 years after it transferred into the Department, ATF never submitted a semiannual report to DOJ summarizing thefts of government property. The Justice Management Division (JMD) sent follow-up correspondence to ATF in 2005, 2006, and 2007 reminding it to submit the semiannual reports, but ATF never submitted the required reports. An ATF official told us that ATF never submitted the semiannual reports because the property management system did not allow ATF to consolidate the loss information. He further stated that ATF is in the process of updating its property management system so that it will be able to consolidate loss information in the future. We have asked JMD about this response and are awaiting its answer. Moreover, in our judgment, ATF could have prepared the required semiannual reports using ATF Reports of Survey.

## *Department of Justice Computer Emergency Response Team*

Since March 2005, DOJ has required all components, including ATF, to submit immediate reports summarizing incidents involving the loss of both classified and unclassified systems to DOJCERT. DOJCERT assists in handling computer security incidents throughout DOJ. ATF also requires such incidents to be reported to its Internal Affairs office.

We used the incidents reported to Internal Affairs to determine if all incidents of lost, stolen, or missing laptop computers reported internally to ATF had been reported to DOJCERT. We identified 53 laptop computer losses that were reported to Internal Affairs, of which 16 occurred prior to the DOJCERT reporting requirement, leaving 37 incidents that should have been reported. We found that 21 of the 37 had been reported to DOJCERT, while 16 were not reported as required.

As of July 2008, we had not received a response from ATF on the reasons why those 16 laptop computers were not reported to DOJCERT. Reporting of these incidents is an important step to ensure that appropriate actions can be taken as soon as possible to mitigate the consequences of laptop computer losses.

### *Disposed Weapon and Laptop Computer Records*

We reviewed a sample of records of ATF disposed weapons and laptop computers to determine if the dispositions were supported by appropriate documentation. Weapons and laptop computers recorded in the property management system as disposed include items that are destroyed, transferred to another agency, lost, stolen, exchanged, donated, or returned. Weapons and laptop computers that are identified as missing during a physical inventory are also removed from active status in ATF's property management system and recorded as disposed items.

We examined whether records for each of the sampled 297 weapons and laptop computers included the proper support documentation and whether each document contained the appropriate authorizations for each disposal. Our review found that ATF was unable to provide documentation supporting proper disposition for 5 (5 percent) of 99 disposed weapons and 21 (12 percent) of 170 disposed laptop computers.

Officials at the ATF Materiel Management office told us that the records supporting the removal of all 5 unsupported weapons and 10 of the

21 unsupported laptop computers from the active property records were misplaced when ATF moved to its new headquarters building in August 2007. In addition, two laptop computer disposals did not include all required signatures and nine did not have the Property Identification Numbers listed on the disposal documents.

Not "clearing" data on laptop computers prior to disposal exposes ATF to security risks. Before laptop computers are disposed of, ATF policy requires the property custodian and the property accountable officer to ensure that hard drives are cleared and a Certificate of Data Clearing is prepared. However, ATF could only provide these certificates for 4 (3 percent) of 116 laptop computers we tested. While ATF officials told us they believe that most of the hard drives were cleared of data, the data clearing status for 97 percent of the disposed laptop computers was not documented and therefore could not be confirmed.

#### *Exit Procedures for Departing Employees*

On or before an employee's last day of employment, an ATF supervisor or other designated official is required to collect property issued to the employee, including weapons, ammunition, and laptop computers. The supervisor is supposed to complete and sign a separation checklist, and provide copies to the employee and the personnel office.

We requested the separation checklists and property information for a sample of 30 former employees. ATF could provide only 6 of the 30 separation checklists, and we found no information on the 6 separation checklists specifying the property being returned. The separation checklist provided to us includes only a statement certifying that the supervisor received all property from the separating employee. In addition, ATF's property management system does not allow a query to determine the property that the separating employee possessed.<sup>25</sup> As a result, ATF has no documentation showing whether all of the property assigned to separating employees has been recovered. Consequently, we were unable to test to ensure that separating employees returned all weapons and laptop computers prior to their separation from ATF service.

---

<sup>25</sup> We were not able to use the property management system to identify items associated with each separating employee because names are not recorded in a standard format and no other identifiers, such as employee numbers are used.



## **Internal Controls Over Ammunition**

In 2002, the Treasury OIG reported that ATF had limited written policies regarding controls over ammunition, no standard recordkeeping, and no physical inventories. As a result of the Treasury audit, in May 2002 ATF issued new policies in ATF Memorandum 1851, Ammunition Inventory, requiring ATF divisions to perform an annual inventory – assisted by a “disinterested person” – of all ATF-owned ammunition and to maintain a perpetual inventory system for ammunition.

We sought to review the last two annual ammunition inventories. However, we were unable to perform the review because ATF could not produce documentation from any ammunition inventories. As of July 2008, ATF officials had not provided us with the required documentation, and have not directly answered why they cannot provide the documentation.

We also reviewed ammunition at 20 ATF offices where we tested weapons and laptop computers. Of the 20 offices, we found that 11 maintained perpetual inventory records for ammunition, as required, and 9 did not. For the 11 offices that maintained perpetual records, the records in 5 of the offices were accurate regarding ammunition, while the records in the 6 other offices contained inaccuracies. One of those 6 offices had significant inaccuracies in all but one type of ammunition, including records for one caliber ammunition that undercounted 478,400 rounds. The inventory was apparently not updated as transactions occurred. The official responsible for the ammunition believed the missing ammunition had probably been given to the military. While this may be correct, ATF has no way of verifying what happened to the missing ammunition without a record of the transactions.

The nine offices that did not maintain perpetual inventories and the one office that had significant deficiencies in its records did not follow ATF procedures to account for all stored ammunition. For example, an agent in an office that did not keep complete perpetual records said he believed that the requirement to keep the perpetual records had been rescinded, a statement ATF headquarters had not confirmed. As a result of not keeping accurate perpetual records, ATF risks the undetected loss of ammunition.

### *Reconciling Ammunition Records to the Financial System*

During our review, we selected 12 shipments of ammunition to trace from purchase through distribution to ammunition inventories at 8 locations. We were unable to trace any shipment into inventory records at any of the

eight receiving locations. Although ATF policy requires the maintenance of perpetual records, five of the eight locations did not keep ammunition inventory records. At two of the other field offices, records were retained for only the previous year, which did not include the tested shipments. At the headquarters ammunition facility (the eighth location), an agent told us that the shipment may have been intended for the Baltimore office and would not have been recorded on the headquarters facility inventory.

### *Physical Security*

The Treasury OIG's 2002 audit reported that ATF had satisfactory procedures for ensuring the physical security of its ammunition. Our audit concluded that ATF continued to have proper physical security over ammunition. We found that ammunition was stored and secured using various methods depending on the size of the ATF office we tested. Smaller ATF field offices kept ammunition stored in vaults within the office space. The vaults had key card access with alarm systems and only ATF personnel had access to these vaults. Larger field offices and divisions kept ammunition in warehouse facilities or at a firing range. The warehouse facilities stored other equipment items in addition to ammunition.

### **Internal Controls Over Explosives**

The Treasury OIG's 2002 audit reported that ATF controls over the physical inventories of explosives lacked independence because they did not include personnel who were independent of daily responsibility for the explosives. In response to the finding, ATF required that a disinterested person participate in all future inventories of explosives. ATF also mandated that a perpetual record of each type of ATF-owned explosive be maintained.

We reviewed 16 ATF locations and found that each kept perpetual inventory records of explosives as required. At each location, we compared the perpetual records for each type of explosive to the actual inventory stored at the location. We found that eight of the locations had accurate perpetual records and eight had inaccuracies. In addition, ATF's Explosives Industry Operations Section performs annual inspections of all ATF explosives magazines, which include a physical inventory review by "disinterested" persons independent of daily responsibility for the magazines.

We concluded that ATF's controls over explosives were adequate. All offices kept perpetual explosives inventory records as required, each

magazine had an annual independent inspection that included an inventory review by an independent person, and we only found minor discrepancies.<sup>26</sup>

### *Reconciling Explosives Records to the Financial System*

We reviewed the two ATF purchases of explosives that occurred within our audit period, both of which were sent to the ATF's K-9 training facility. We were able to trace both shipments from the invoices to the perpetual log at the training facility. Therefore, we were able to reconcile the purchases of explosives to the explosives inventory.

### *Physical Security*

Storage of explosives is regulated by ATF's Explosives Industry Operations Section. We found explosives storage was uniform among the ATF offices we visited. In ATF Memorandum 5400, ATF required an independent physical security review of all magazines that found all magazines reviewed were secured. Therefore, we concluded that ATF's physical controls over explosives were adequate.

## **Conclusion and Recommendations**

Our audit found significant increases in the ATF's rate of loss for weapons and laptop computers since the Treasury audit was issued in 2002, and the ATF's rate of loss for weapons was nearly double the rates of loss for the FBI and DEA. In addition, ATF staff did not follow established policy to report many lost, stolen, or missing weapons and laptop computers to ATF Internal Affairs, investigate losses, or enter reports of lost, stolen, or missing weapons into NCIC. We also found that ATF did not know whether most of its lost, stolen, or missing laptop computers contained sensitive or classified information.

We concluded that ATF's controls over weapons and laptop computers were not adequate. ATF did not maintain accurate and complete records in its property management system or maintain support documentation for disposed weapons and laptop computers, nor did it document that laptop computer hard drives were cleared prior to disposal. In addition, ATF could not locate all of the active weapons and laptop computers sampled for review. It also did not report to the DOJ CIO the number of laptop computers authorized to process classified information or report all weapon

---

<sup>26</sup> A magazine is a secured storage container for explosives. See the photograph of an explosives magazine in Finding III.

and laptop computer losses to DOJ and all laptop computer loss incidents to DOJCERT, as required. Furthermore, we determined five of ATF's classified laptop computers were not encrypted. In addition, ATF could not provide documentation to show that it received all weapons and laptop computers from separating employees.

We determined that ATF's controls over explosives were adequate. However, we identified continued weaknesses in controls over ammunition. Although ATF had developed written procedures to enhance controls over ammunition in response to the 2002 Treasury audit, ATF failed to enforce its policy to perform annual inventories of ammunition and maintain accurate and complete perpetual ammunition inventory records.

Our audit report makes 14 recommendations for ATF to improve its controls over weapons, laptop computers, and ammunition. The recommendations include that ATF follow established policy to report all weapons, laptop computers, and ammunition losses to Internal Affairs and ensure that all necessary information for investigation is complete and accurate. Also, ATF should ensure that it is able to determine the contents of all lost, stolen, or missing laptop computers. In addition, ATF should maintain accurate and complete records in its property management system. Furthermore, ATF should enforce current requirements to perform annual inventories of ammunition and to maintain accurate and complete ammunition records.

## TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>1</b>
<b>Background.....</b>	<b>2</b>
<b>Property Management .....</b>	<b>6</b>
<b>OIG Audit Approach .....</b>	<b>10</b>
<b>FINDINGS AND RECOMMENDATIONS .....</b>	<b>12</b>
<b>I. ATF'S RESPONSE TO WEAPON, LAPTOP COMPUTER,         AMMUNITION, AND EXPLOSIVES LOSSES .....</b>	<b>12</b>
<b>Rates of Loss.....</b>	<b>14</b>
<b>Circumstances of Lost, Stolen, or Missing Weapons .....</b>	<b>21</b>
<b>Circumstances of Lost, Stolen, or Missing Laptop Computers.....</b>	<b>22</b>
<b>Reporting Weapon and Laptop Computer Losses .....</b>	<b>24</b>
<b>Investigations and Consequences of Losses.....</b>	<b>28</b>
<b>Contents of Lost, Stolen, or Missing Laptop Computers.....</b>	<b>31</b>
<b>Entering Losses into NCIC.....</b>	<b>35</b>
<b>Ammunition and Explosives Losses .....</b>	<b>37</b>
<b>Conclusion.....</b>	<b>39</b>
<b>Recommendations.....</b>	<b>41</b>
<b>II. INTERNAL CONTROLS OVER WEAPONS AND LAPTOP         COMPUTERS .....</b>	<b>42</b>
<b>Physical Inventories.....</b>	<b>42</b>
<b>Reconciling Property Records to the Financial System .....</b>	<b>43</b>
<b>Inaccurate and Incomplete Property Records .....</b>	<b>44</b>
<b>Encryption.....</b>	<b>50</b>
<b>Reporting Requirements for Laptop Computers Containing             Classified Information.....</b>	<b>52</b>
<b>Reporting Losses to DOJ .....</b>	<b>52</b>
<b>Disposal of Weapons and Laptop Computers.....</b>	<b>53</b>
<b>Exit Procedures for Departing Employees .....</b>	<b>58</b>
<b>Conclusion.....</b>	<b>58</b>
<b>Recommendations.....</b>	<b>59</b>
<b>III. INTERNAL CONTROLS OVER AMMUNITION AND EXPLOSIVES... </b>	<b>61</b>
<b>Ammunition Controls .....</b>	<b>61</b>
<b>Explosives Controls .....</b>	<b>66</b>
<b>Conclusion.....</b>	<b>69</b>
<b>Recommendation .....</b>	<b>69</b>
<b>STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS.....</b>	<b>70</b>

**APPENDICES:**

<b>I.</b>	<b>OBJECTIVES, SCOPE, AND METHODOLOGY.....</b>	<b>71</b>
<b>II.</b>	<b>SAMPLING DESIGN .....</b>	<b>74</b>
<b>III.</b>	<b>CIRCUMSTANCES OF WEAPON LOSSES REPORTED TO INTERNAL AFFAIRS.....</b>	<b>76</b>
<b>IV.</b>	<b>CIRCUMSTANCES OF LAPTOP COMPUTER LOSSES REPORTED TO INTERNAL AFFAIRS.....</b>	<b>82</b>
<b>V.</b>	<b>ANALYSIS OF LOST, STOLEN, OR MISSING WEAPONS REPORTED TO INTERNAL AFFAIRS.....</b>	<b>86</b>
<b>VI.</b>	<b>ANALYSIS OF LOST, STOLEN, OR MISSING LAPTOP COMPUTERS REPORTED TO INTERNAL AFFAIRS.....</b>	<b>88</b>
<b>VII.</b>	<b>ANALYSIS OF PROPERTY MANAGEMENT RECORDS.....</b>	<b>90</b>
<b>VIII.</b>	<b>LOST, STOLEN, OR MISSING WEAPONS AND LAPTOP COMPUTERS REPORTED TO INTERNAL AFFAIRS BY ATF FIELD OFFICE .....</b>	<b>91</b>
<b>IX.</b>	<b>AMMUNITION CONTROL LOG .....</b>	<b>92</b>
<b>X.</b>	<b>EXPLOSIVES CONTROL LOG .....</b>	<b>93</b>
<b>XI.</b>	<b>ORGANIZATIONAL CHART .....</b>	<b>94</b>
<b>XII.</b>	<b>ATF FORM 1851.3, REPORT OF SURVEY.....</b>	<b>95</b>
<b>XIII.</b>	<b>ACRONYMS AND ABBREVIATIONS.....</b>	<b>96</b>
<b>XIV.</b>	<b>THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES' RESPONSE TO THE DRAFT REPORT .....</b>	<b>97</b>
<b>XV.</b>	<b>OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT .....</b>	<b>105</b>

## INTRODUCTION

The U.S. Department of Justice (DOJ) Office of the Inspector General (OIG) performed a series of audits in 2002 that examined controls over weapons and laptop computers in four DOJ components – the Federal Bureau of Prisons, Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), and United States Marshals Service.<sup>1</sup> The Attorney General requested these audits in response to concerns raised in an OIG audit report about the potentially serious consequences of losing such sensitive property.<sup>2</sup> The 2002 audits found substantial losses and weak controls over management of this property throughout the DOJ.

At the time the 2002 weapon and laptop computer audits were performed, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) was part of the Department of the Treasury (Treasury) and not a component of DOJ. The Homeland Security Act subsequently transferred the law enforcement functions of ATF into DOJ on January 24, 2003.

In 2002, Treasury's Office of Inspector General (OIG) issued an audit of ATF's controls over sensitive property, which included firearms, computers, ammunition, and explosives.<sup>3</sup> The audit found that ATF had adequate controls over firearms and laptop computers and generally took appropriate actions in response to lost, stolen, or missing property, but that controls over ammunition and explosives needed improvement. The Treasury audit specifically cited the lack of periodic inventories of ammunition and inadequate inventory records of explosives. The audit also found that explosives inventories were not conducted with adequate independence because persons outside the chain-of-custody for explosives did not witness periodic physical inventories. ATF concurred with the findings and recommendations and reported that it had implemented new controls to address the weaknesses.

In response to the 2002 Treasury audit, ATF required all divisions to conduct a baseline ammunition inventory and report the results to ATF

---

<sup>1</sup> U.S. Department of Justice Office of the Inspector General, *The Department of Justice's Control Over Weapons and Laptop Computers Summary Report*, Audit Report 02-31 (August 2002).

<sup>2</sup> U.S. Department of Justice, Office of the Inspector General, *Immigration and Naturalization Service Management of Property*, Audit Report 01-09 (March 2001).

<sup>3</sup> U.S. Department of the Treasury, Office of Inspector General, *Protecting the Public: Bureau of Alcohol, Tobacco and Firearms' Control over Sensitive Property is Adequate*, Audit Report 02-097 (June 2002).

headquarters. ATF also implemented policies requiring that all divisions perform an annual 100-percent inventory of all ATF-owned ammunition, persons outside the chain-of-custody for explosives participate in all future inventories of ATF explosives magazines, and divisions maintain perpetual records for each type of ATF-owned explosive.<sup>4</sup>

## **Background**

ATF is responsible for enforcing federal criminal laws and also for regulating the firearms and explosives industries. ATF has headquarters divisions located in the Washington, D.C., and Martinsburg, West Virginia area; training facilities located in Glynco, Georgia, Front Royal, Virginia, and Fort A.P. Hill, Virginia; and approximately 250 field and satellite offices within 25 field divisions that are divided into the Eastern, Central, and Western regions across the country.<sup>5</sup> ATF also has personnel located in several foreign countries. The following graphic displays the geographic distribution of ATF field divisions. ATF personnel located in other countries are not reflected in the graphic.

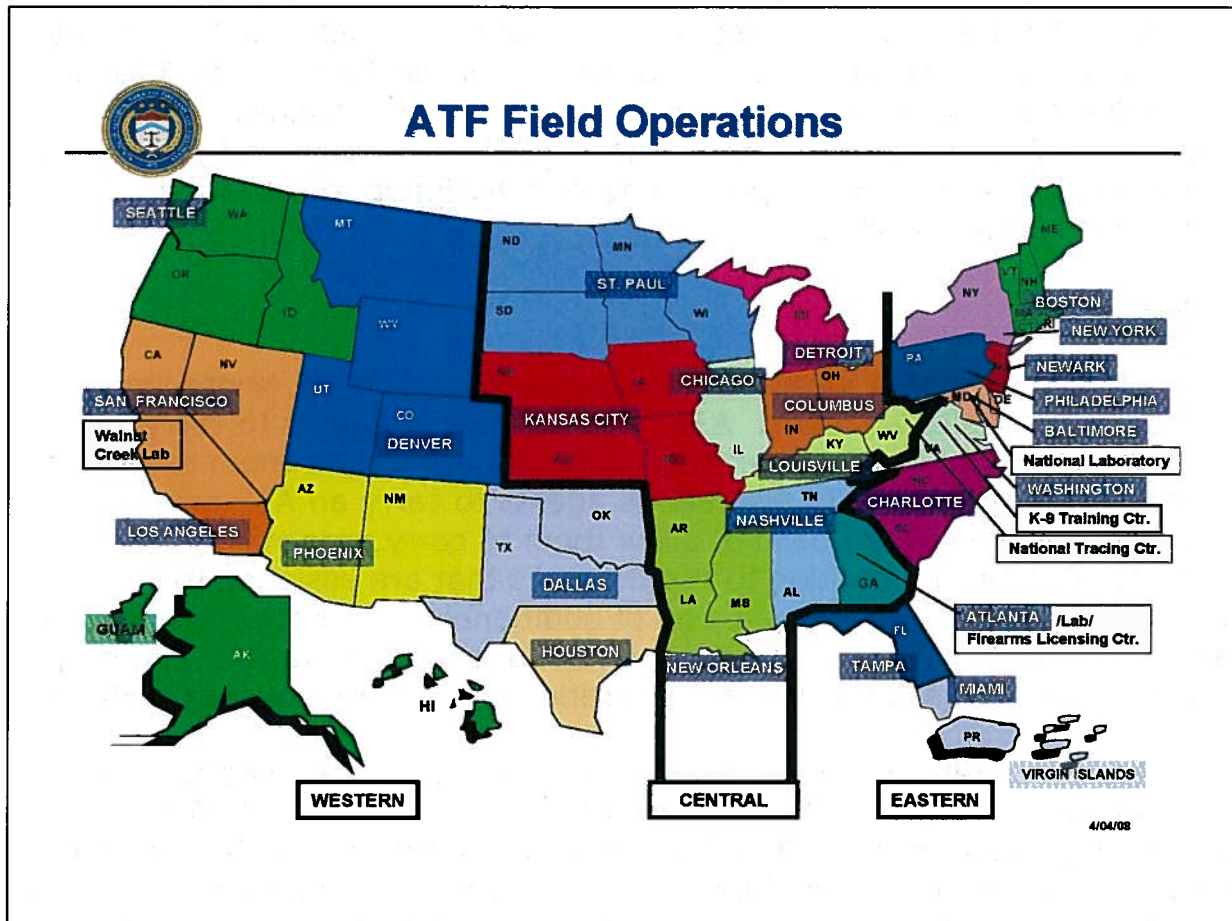
---

<sup>4</sup> A magazine is a secured storage container for explosives. See the photograph of an explosives magazine in Finding III. Perpetual inventory is an inventory accounting system in which book inventory is updated continuously, as opposed to periodic inventories in which updates are made on a recurring basis, such as annually.

<sup>5</sup> At the beginning of our review in July 2007, ATF had 23 field divisions. In December 2007 and April 2008, ATF added two additional field divisions in Denver, Colorado, and Newark, New Jersey. Denver was previously a field office within the Phoenix Field Division and Newark was a field office within the New York Field Division.



## ATF DIVISIONS MAP



Source: ATF website

ATF is led by a Director and Deputy Director, and each region has a Deputy Assistant Director. Each headquarters division is led by a Chief and each field division has a Special Agent in Charge (SAC). An organizational chart listing ATF's divisions is located in Appendix XI.

Among ATF's major headquarters directorates are the Office of Management (OM) and the Office of Professional Responsibility and Security Operations (OPRSO). The Office of Management includes the Materiel Management Branch that oversees property management.<sup>6</sup> OPRSO includes the Internal Affairs Division (Internal Affairs), which investigates property losses as those relate to employee misconduct.

<sup>6</sup> "Materiel" is a term used to refer to equipment and supplies, especially in military organizations, which is also used by the ATF.

As of August 2007, ATF employed 2,461 Special Agents, 1,095 Explosives Industry Operations Investigators, and 1,289 other support personnel. Special Agents investigate criminal cases, Industry Operations Investigators conduct onsite investigations and inspections of the firearms and explosives industries, and support personnel help administer ATF programs and operations. As of August 17, 2007, ATF reported that it had 22,476 weapons and 7,505 laptop computers assigned to staff in its domestic and foreign offices.<sup>7</sup>

### *Weapons*

ATF's inventory of weapons included handguns, rifles, shotguns, tasers, and specialty weapons. ATF requires Special Agents to carry an ATF-owned primary handgun while on duty and authorizes them to carry the weapon while off duty. ATF also allows agents to carry an ATF-owned secondary handgun, but does not allow them to carry personally-owned weapons on duty. In addition to the weapons that are assigned to Special Agents, ATF maintains a pool of additional weapons for assignment and use as needed. The pool consists of rifles, shotguns, tasers, and prop weapons that are used for training, operations, and undercover operations.<sup>8</sup>

Approximately one-third of ATF's 22,476 weapons are maintained in a reference collection at the ATF Firearms Technology Branch (FTB) in Martinsburg, West Virginia. The FTB uses the reference collection to test, evaluate, and provide expert testimony on firearms and ammunition. It also uses the collection to provide technical services to the firearms industry and other members of the public. According to a former chief of the FTB, the reference collection was established in the late 1960's. At the time of our audit, the reference collection included seized weapons, weapons of historical significance, homemade weapons, and weapons modified from household items such as umbrellas, belt buckles, and writing pens.

### *Laptop Computers*

ATF assigns laptop computers to Special Agents, Industry Operations Investigators, other ATF employees, contractors, and Task Force Officers who work for other law enforcement agencies. ATF personnel use laptop computers to prepare investigative reports, access various law enforcement

---

<sup>7</sup> See Appendix VII for an analysis of ATF's assigned weapons and laptop computers.

<sup>8</sup> During an undercover operation, an ATF undercover agent can show the prop weapon as merchandise to a person wanting to purchase a weapon illegally.

databases, support electronic surveillance activities, and complete administrative tasks.

ATF leases laptop computers rather than purchasing them outright. ATF replaces laptop computers every 3 years, at which time most of the laptop computers are disposed of and replaced by new leased computers.<sup>9</sup> However, ATF retains ownership of the replaced laptop computers and maintains a few of the computers after the lease has expired to use for special purposes, such as Global Positioning System (GPS) tracking and video surveillance.

During our audit, ATF reported that 18 of its 7,505 laptop computers were authorized to process classified information. Five of the 18 laptop computers were located at ATF headquarters in Washington, D.C., and the remaining 13 were assigned to offices of the ATF Explosives Technology Branch (ETB) located in various cities.

### *Ammunition*

Each ATF field division and headquarters law enforcement division maintains a supply of ammunition. The ammunition consists of various types, including .40 caliber, 9 millimeter (mm), .223 Remington, and 12 gauge. Most ammunition is used for weapons qualification and training.

### *Explosives*

ATF houses explosives in secured storage containers called magazines throughout the United States. ATF personnel in the field, headquarters, and training divisions maintain the magazines and account for the explosives. Each magazine contains multiple types of explosives, including Composition-4 (C-4), detonation cord, and blasting caps.<sup>10</sup> ATF uses explosives for training and field operations.

---

<sup>9</sup> This represents a refresh cycle of 3 years that is normal in the information technology industry.

<sup>10</sup> C-4 is a common variety of military plastic explosive. Detonation cord is a thin, flexible tube with an explosive core. Blasting caps are small explosive device generally used to detonate a larger, more powerful explosive such as dynamite.

## Property Management

Office of Management and Budget (OMB) 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.<sup>11</sup> The Justice Property Management Regulations require that DOJ components issue detailed operating procedures to protect federal property against fraud, waste, and abuse.<sup>12</sup>

ATF Order 1850.2C, Property Management Program, dated November 8, 2001, contains ATF guidelines for the general management of property.<sup>13</sup> According to these guidelines, all ATF employees are responsible for the proper care and protection of government property they use and control and may be held financially responsible for its loss.

ATF staff told us that all weapons and laptop computers are recorded in the property management system. Ammunition and explosives are considered to be expendable supply items and are not subject to recording as ATF property in the property management system.

### *Property Management Organization*

According to ATF's property management policy, responsibility for property management is shared by a property management officer and a property accountable officer at ATF headquarters, and property management representatives and property custodians assigned to each headquarters and field division office. Their responsibilities are outlined below.

- The property management officer is responsible for the general managerial oversight of ATF's property management program. The Chief of the Materiel Management Branch serves as property management officer.

---

<sup>11</sup> Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control.

<sup>12</sup> DOJ Order 2400.3, Justice Property Management Regulations.

<sup>13</sup> ATF revised this order and issued a new version, ATF Order 1850.2D, effective April 29, 2008.

- The property accountable officer is responsible for ATF's property management system and the authority to delegate responsibility for the physical control of property. The property accountable officer is responsible for the receipt, utilization, and disposal of ATF property. The Chief of the Property and Fleet Management Section, within the Materiel Management Branch, serves as the property accountable officer.
- Property management representatives are responsible for the accuracy and certification of the property inventories pertinent to their accounts and for ensuring that Property Issue Receipts are maintained for all property assigned to individuals. The representatives are also responsible for initiating investigative action pursuant to the damage or loss of ATF property. Within each field division or headquarters unit, the Division Director, SAC, Resident Agent in Charge, Area Supervisor, or Group Supervisor serves as the property management representative.
- Property custodians are responsible for the receipt, physical distribution, and control of all property located in their assigned areas. The custodians maintain Property Issue Receipts for all property issued to individuals within their areas. The property management representative designates a property custodian for each division.

In addition to support from the field personnel identified above, other parts of ATF coordinate with the Materiel Management Branch to ensure control over ATF property and information on laptop computers. These organizations include the Internal Affairs Division, which investigates property losses as those relate to employee misconduct; and the Office of Science and Technology, which manages laptop computers.

### *Automated Property Management System*

ATF uses a commercial-off-the-shelf automated property management system that provides a variety of functions to record information and assign property. The system is designed to:

- record detailed asset information;
- organize and track ownership;
- provide information about costs, installed components, service history, and current value of property;

- generate reports that reflect the status of property; and
- maintain consistency and accuracy in property reporting.

ATF limits access to the property management system to ATF Materiel Management staff at headquarters and property custodians in the field. Only Materiel Management staff is able to add and remove items from the system. Property custodians can only accept or transfer items within their Divisions. The Chief of the Property and Fleet Management Section told us that the system included about 92,000 items as of March 2008. In addition to weapons and laptop computers, the system also accounts for items such as printers, scanners, and vehicles.

#### *Procedures for Lost, Stolen, or Missing Property*

The procedures for reporting lost, stolen, or missing property are outlined in DOJ property management regulations and information technology security standards, ATF property management policies, and in Office of Management and Budget memoranda.

Section 128-51.102 of DOJ Order 2400.3, Justice Property Management Regulations, requires that any incidents of loss, theft, damage, destruction, or other conditions adversely affecting personal property be reported to the property management officer. Further, the property management officer is to refer incidents to a board of survey or other internal review organization for investigations. Incidents not referred are subject to a less formal administrative review. However, inconclusive reviews and recurring irregularities in a single location or property account are to be referred for formal investigation to a board of survey.

ATF property management policy requires lost, stolen, or missing weapons be entered into the National Crime Information Center (NCIC). NCIC is a database of criminal justice information, such as criminal record history, fugitives, stolen property, and an index of individuals incarcerated in the federal prison system. Criminal justice agencies enter records into NCIC, and those records are then accessible to law enforcement agencies nationwide. The NCIC system is generally regarded by law enforcement agencies as the primary method for tracking stolen or recovered weapons. Failure to timely enter items into NCIC could reduce the chance of recovering the weapon or laptop computer or identifying whether the weapon was used in the commission of a crime. In April 2008, ATF revised its property management policy to require that laptop computers containing classified information also be reported to NCIC.

ATF's property management policy also requires employees who lose their assigned property to immediately report the loss or theft to the property custodian, property management representative, and Special Agent in Charge, division director, or chief. The property management representative is required to obtain the circumstances and all known facts surrounding the incident and prepare a memorandum to report the lost, stolen, or missing property to the property accountable officer within 10 working days from the date of the incident. The property management representative is then required to report the loss or theft to the property accountable officer.

Once the property accountable officer receives the report of the loss or theft, he or she should prepare an ATF Form 1851.3, Report of Survey, and forward it, along with any memorandum and any other necessary attachments, such as a police report, to a designated deciding official.<sup>14</sup> The deciding official's designation is based on the chain of command of the individual responsible for the property at the time of the incident.

The property accountable officer removes lost property from the property management system and maintains a file of the Reports of Survey.<sup>15</sup> The property accountable officer also provides a copy of the Report of Survey to Internal Affairs for review and action, as deemed necessary.<sup>16</sup>

In March 2005, DOJ issued Information Technology Security Standard 2.9 requiring that all DOJ components report computer incidents involving classified and unclassified systems to the Department of Justice Computer Emergency Response Team (DOJCERT). In December 2006, the Department revised this policy and outlined additional reporting requirements, including

---

<sup>14</sup> A Report of Survey (ATF Form 1851.3) is used to document the loss, theft, damage, or destruction of government-owned or government-leased property that is not caused by normal wear and tear or intentional destruction of property. The Report of Survey is used to adjust property accounting records.

<sup>15</sup> ATF policy only specifies this step for lost property, but we believe the intent of the policy is to include all lost, stolen, or missing property in this part of the procedure.

<sup>16</sup> Originally, ATF policy stated that the Report of Survey was to be provided to the Director for the ATF Office of Inspections. In July 2004 ATF changed the name of Office of Inspections to the Office of Professional Responsibility and Security Operations (OPRSO). ATF revised this policy and issued a new version, ATF Order 1850.2D, effective April 29, 2008, that includes the name change.

requirements for reporting the loss of personally identifiable information (PII).<sup>17</sup> ATF's policies did not include the DOJCERT reporting requirements because ATF last updated its policy in 2001, prior to the issuance of the DOJCERT standard in 2005. However, in April 2008 ATF revised its policies but still did not include the DOJCERT reporting standard. Nonetheless, some lost, stolen, or missing laptop computers were, in fact, reported to DOJCERT.

ATF's property management policy does not require an assessment of whether or not a lost, stolen, or missing laptop computer contained sensitive or classified information. ATF officials told us that ATF had an unwritten policy requiring that a user be interviewed about the contents of a lost, stolen, or missing laptop computer when it was reported missing.

### **OIG Audit Approach**

We conducted this audit to assess ATF's controls over weapons, laptop computers, ammunition, and explosives. We interviewed ATF officials, reviewed documents, and tested controls at:

- headquarters division offices in metropolitan Washington, D.C. and Martinsburg, West Virginia;
- field divisions in Atlanta, Georgia; Kansas City, Missouri; Los Angeles, California; New Orleans, Louisiana; Philadelphia, Pennsylvania; San Francisco, California; and Washington, D.C.; and
- training facilities at Glynco, Georgia; Fort A.P. Hill, Virginia; and Front Royal, Virginia.

Our audit examined actions taken in response to the identification of lost, stolen, or missing weapons and laptop computers and assessed whether ATF staff followed current procedures. We also queried NCIC to determine whether lost, stolen, or missing weapons were entered into the database and to identify weapons that were recovered or used in the commission of a crime. We address these issues in Finding I.

---

<sup>17</sup> According to Office of Management and Budget (OMB) Memorandum M-07-16, dated May 22, 2007, PII 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 name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to an individual.



We reviewed the ATF'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. Our results of these analyses are found in Finding II.

We also reviewed controls over ammunition and explosives to determine whether ATF stored and accounted for these items properly. Our results of these analyses are found in Finding III.

## **FINDINGS AND RECOMMENDATIONS**

### **I. ATF'S RESPONSE TO WEAPON, LAPTOP COMPUTER, AMMUNITION, AND EXPLOSIVES LOSSES**

During our 59-month review period, ATF reported 76 weapons and 418 laptop computers as lost, stolen, or missing, including 7 laptop computers that contained sensitive information. Of the 76 weapons, 35 were reported as stolen, 19 were reported as lost, and 12 were reported as missing during periodic inventories. ATF was unable to document what happened to the 10 additional weapons.

Of the 418 lost, stolen, or missing laptop computers, 274 were identified as missing during periodic inventories, 50 were reported as stolen, and 8 were reported as lost. ATF could not provide information about the remaining 86 lost, stolen, or missing laptop computers because the records had been destroyed in accordance with ATF's record retention cycle or could not be found.

We found that ATF investigated laptop computer losses reported to Internal Affairs but did not investigate most laptop computer losses because they were not reported to Internal Affairs. ATF officials could not provide documentation showing whether 398 of the 418 lost, stolen, or missing laptop computers contained sensitive or classified information.

In addition, ATF did not consistently enter all lost, stolen, or missing weapons into the National Crime Information Center (NCIC) database as required. ATF made preliminary investigations into all reported losses of ammunition and explosives and found no employee misconduct.

We interviewed ATF officials, reviewed policies and investigative reports, and obtained and analyzed property records to determine the number of weapons and laptop computers lost, stolen, or missing between October 1, 2002, and August 31, 2007. We found that 76 weapons and 418 laptop computers were lost, stolen, or missing during this 59-month period.

Of the 76 weapons, 35 were reported stolen, 19 were reported lost, and 12 were reported missing. ATF was unable to document what occurred in the other 10 cases.

Of the 418 laptop computers, 50 were reported stolen, and 8 were reported lost. We could not specifically determine whether 86 laptop computers were lost, stolen, or missing because the records had been destroyed or were not found.

The remaining 274 laptop computers are those that ATF officials identified as missing during periodic inventories.<sup>18</sup> While ATF officials offered several explanations for these items, they were unable to document adequately the circumstances or dispositions of the 274 missing laptop computers, and we included them in our totals of lost, stolen, or missing laptop computers.<sup>19</sup> Further details about the lost, stolen, or missing items are included throughout this finding.

To investigate the 274 laptop computers reported as missing, we interviewed property management officials and reviewed property management policies and the documented results of periodic ATF inventories. Officials told us the contractor that leases laptop computers to ATF provided an electronic list of laptop computers that were scheduled for shipment to various offices and ATF staff used that list to update its property records electronically. However, according to ATF officials, many of those laptop computers were sent to other locations.<sup>20</sup> As a result, ATF officials said the property records were incorrect. In June 2004, ATF created a separate account in its property management system to account for the pool of laptop computers belonging to the contractor that have yet to be issued to ATF employees.

---

<sup>18</sup> As of January 2008, 271 of 274 laptop computers ATF identified as missing during inventories had been removed from the active property records.

<sup>19</sup> One ATF official said the laptop computers were not missing and that we should report those items as "inventory discrepancies." Other ATF officials believed those laptop computers had been donated, transferred, or returned to the contractor but could not provide the supporting documentation. We categorize these items as lost because ATF cannot document the circumstances surrounding their "missing" status and cannot document the disposition of the items. We treated these items similarly in our FBI and DEA audits.

<sup>20</sup> ATF staff did not provide information about exactly when this occurred.

We also reviewed documentation of inventory results submitted to ATF headquarters. Those documents explain that field offices at one time had the missing laptop computers in their possession but the disposition of those laptop computers was not documented. For example, one field office official believed 31 laptop computers that could not be located during an annual inventory had been returned to the contractor without the associated paperwork. Another field office official believed 29 laptop computers were missing due to the contractor's failure to provide paperwork when removing or replacing the laptop computers. Other field office officials believed the laptop computers were "missing" due to donations and computer refreshes that were not documented. However, without documentation there is no way of knowing what happened to those "missing" laptop computers.

These explanations could be the causes for the large number of laptop computers identified as missing during periodic ATF inventories. It appears that ATF did not adequately oversee the contractor responsible for managing the laptop computers and did not ensure that exchanges, transfers, and donations of property were properly documented and processed in a timely manner to adjust the property records or remove those items from the records. However, because ATF could not provide documentation to support these explanations we included the 274 missing laptop computers in our analysis.

### **Rates of Loss**

For perspective on the 76 weapons and 418 laptop computers included in our category of lost, stolen, or missing, we developed loss rates to compare with losses previously reported for ATF and with those experienced by other DOJ components. Comparable information is contained in the 2002 Treasury audit report and in OIG audit reports for the FBI and DEA.

To compare losses during our 59-month audit period with Treasury's 2002 audit findings, we calculated losses per month because the audit periods were different lengths.<sup>21</sup> We determined that ATF's rates of loss for both weapons and laptop computers had increased substantially since the 2002 Treasury audit report. The following table shows the total losses and losses per month for both weapons and laptop computers for both audits. The two right columns compare the losses per month between our audit

---

<sup>21</sup> The 2002 Treasury OIG audit covered the 36-month period from October 1, 1998, through September 30, 2001. The current audit covered the 59-month period from October 1, 2002, to August 31, 2007.

period and the period covered by the 2002 Treasury audit. The 1.29 weapons lost per month for our audit period was nearly three times the 0.47 weapons lost per month reported by Treasury in 2002. The 7.08 laptop computer losses per month for our audit period were approximately 50 times the 0.14 computer losses per month reported by Treasury OIG.

**LOST, STOLEN, OR MISSING WEAPONS AND LAPTOP COMPUTERS  
2002 TREASURY OIG AUDIT VS. CURRENT DOJ OIG AUDIT**

<b>Category</b>	<b>Number of Lost, Stolen, or Missing Items Reported</b>		<b>Losses Reported Per Month</b>	
	<b>2002 Audit (36-month period)</b>	<b>Current Audit (59-month period)</b>	<b>2002 Audit</b>	<b>Current Audit</b>
Lost weapons	4	19	0.11	0.32
Stolen weapons	13	35	0.36	0.59
Weapons identified as missing during an inventory	0	12	0.00	0.20
Weapons which could not be categorized as either lost, stolen, or missing because of documents had been destroyed or could not be found	0	10	0.00	0.17
<b>Lost, Stolen, or Missing Weapons</b>	<b>17</b>	<b>76</b>	<b>0.47</b>	<b>1.29<sup>22</sup></b>
Lost laptop computers	0	8	0.00	0.14
Stolen laptop computers	0	50	0.00	0.85
Laptop computers identified as missing during an inventory	0	274	0.00	4.64
Laptop computers which could not be categorized as lost, stolen, or missing because documents had been destroyed or could not be found	5	86	0.14	1.46
<b>Lost, Stolen, or Missing Laptop Computers</b>	<b>5</b>	<b>418</b>	<b>0.14</b>	<b>7.08<sup>23</sup></b>

Source: OIG analysis of ATF data

All of the items included in the table were reported within ATF as lost, stolen, or missing during a periodic physical inventory conducted by ATF

<sup>22</sup> The column does not add up to 1.29 due to rounding.

<sup>23</sup> The column does not add up to 7.08 due to rounding.

staff.<sup>24</sup> Lost and stolen weapons and laptop computers are discussed later in the report. When items are identified as lost, stolen or missing, either during an inventory or otherwise, ATF staff must prepare "Reports of Survey" to explain the losses. We used the Reports of Survey and the Internal Affairs investigative reports to categorize the items summarized in the preceding table.

Some but not all of the lost, stolen, or missing items were reported to ATF Internal Affairs, which prepared investigative reports regarding the circumstance of the loss. Of the 76 lost, stolen, or missing weapons, 63 were reported to Internal Affairs. Of the 418 lost, stolen, or missing laptop computers, 53 were reported to Internal Affairs.<sup>25</sup>

The table shows that 12 weapons were identified as missing during a physical inventory. The 12 missing weapons represent approximately 16 percent of the total lost, stolen, and missing weapons. Investigative reports at Internal Affairs indicated that six of the missing weapons were later recovered.

We compared ATF's missing weapons with those identified as missing during our prior audits of the DEA and FBI. At the DEA, 4 (4 percent) of 91 lost, missing, or stolen weapons were identified as missing during an inventory. At the FBI, 23 (14 percent) of 160 lost, missing, or stolen weapons were identified as missing during an inventory. ATF's percentage of weapons missing during an inventory (16 percent) is higher than the DEA's percentage and about the same as the FBI's percentage.

The table also shows 274 ATF laptop computers were identified as missing during periodic inventories. These losses represent approximately 66 percent of all lost, stolen, or missing ATF laptop computers. The inventory documentation submitted to ATF headquarters provided a variety of reasons for the missing computers. The primary reason was that managers believed the computers were returned to the supplier, exchanged for newer models, or donated to schools after becoming obsolete. However, managers could not demonstrate this had occurred because they could not

---

<sup>24</sup> There is no overlap between items between the categories.

<sup>25</sup> Laptop computers identified as missing during an inventory were generally not reported to Internal Affairs. For weapons, we could not determine the circumstances for weapons not being reported because ATF could not provide documentation about 10 of the 13 weapons not reported to Internal Affairs. The other three were reported missing on Reports of Survey and were treated as inventory adjustments.

produce the required documentation for such returns, exchanges, or donations. Consequently, we include these items in our analysis as missing, which is how we treated this issue in our DEA and FBI audits.

We compared the percentage of ATF's missing laptop computers with those identified as missing during our prior audits of the DEA and FBI. At the DEA, 149 (65 percent) of 231 lost, stolen, or missing laptop computers were identified as missing during an inventory. At the FBI, 62 (39 percent) of 160 lost, stolen, or missing laptop computers were missing during an inventory. ATF's percentage of laptop computers missing during an inventory (66 percent) is nearly equal to the percent missing at the DEA and higher than the percent missing at the FBI.

For 10 of the 76 lost, stolen, or missing weapons and for 86 of the 418 lost, stolen or missing laptop computers, the Reports of Survey had been destroyed at the end of the required record-retention period or were otherwise missing and no investigation reports were prepared.<sup>26</sup> Consequently, we could not determine how these losses should be categorized – lost, stolen, or missing.

### *Comparison of Loss Rates*

To compare ATF's losses with those reported in audits of weapons and laptop computers at the FBI and DEA, we also calculated rates of loss per 1,000 agents because the components vary widely in number of employees. As the following table shows, for our 59-month audit period, ATF's rate for lost, stolen, or missing weapons (.52) was nearly double those of the FBI (.29) and DEA (.28).<sup>27</sup> ATF's losses of laptop computers were significantly higher at nearly 3 per 1,000 agents, compared with less than 1 per 1,000 FBI or DEA agents.<sup>28</sup> The following table shows the loss rates reported in audit reports for these three DOJ components.

---

<sup>26</sup> We know from the property management system that these items were removed based on Reports of Survey. ATF staff told us the records for 8 of the 10 weapons and for 78 of the 86 laptop computers were destroyed in accordance with ATF's written policy that personal property records are to be destroyed 3 years after the property is disposed of. ATF staff could not locate the other records. In Finding I, we discuss concerns regarding reporting items to Internal Affairs.

<sup>27</sup> Of the 76 lost, stolen, or missing weapons our audit identified, 12 (16 percent) were documented as missing during periodic inventories.

<sup>28</sup> The number of lost laptop computers for all 3 components included items identified during periodic inventories as missing.



**LOST, STOLEN OR MISSING WEAPONS AND LAPTOP COMPUTERS  
PER MONTH PER 1,000 AGENTS - ATF, FBI and DEA**

	<b>ATF</b>	<b>FBI</b>	<b>DEA</b>
<b>Number of Agents</b>	2,461	12,515	4,929
<b>Number of Months in Audit Scope</b>	59	44	66
<b>WEAPONS</b>			
<b>Lost, Stolen or Missing</b>	76	160	91
<b>Rate of Loss Per Month Per 1,000 Agents<sup>29</sup></b>	<b>0.52</b>	<b>0.29</b>	<b>0.28</b>
<b>LAPTOP COMPUTERS</b>			
<b>Lost, Stolen, or Missing</b>	418	160	231
<b>Rate of Loss Per Month Per 1,000 Agents</b>	<b>2.88</b>	<b>0.29</b>	<b>0.71</b>

Source: OIG analysis of ATF, FBI, and DEA data

In the following table we show rates of loss per month per 1,000 agents for only those weapons and laptop computers reported stolen. As shown in the table, ATF's rate of loss for stolen weapons (.24) was only slightly higher than the FBI (.17) and DEA (.21) rates of loss. The DEA has a policy that prohibits agents from storing their weapons in vehicles. The ATF and FBI have no such policy. For stolen laptop computers, ATF's rate of loss per month per 1,000 agents (.34) was four times higher than the FBI (.08) and DEA (.08).

**STOLEN WEAPONS AND LAPTOP COMPUTERS  
PER MONTH PER 1,000 AGENTS - ATF, FBI and DEA**

<b>STOLEN WEAPONS AND LAPTOP COMPUTERS</b>	<b>ATF</b>	<b>FBI</b>	<b>DEA</b>
<b>Number of stolen weapons reported</b>	35	94	69
<b>Rate of Loss Per Month Per 1,000 Agents</b>	<i>0.24</i>	<i>0.17</i>	<i>0.21</i>
<b>Number of stolen laptop computers</b>	50	44	25
<b>Rate of Loss Per Month Per 1,000 Agents</b>	<i>0.34</i>	<i>0.08</i>	<i>0.08</i>

Source: OIG analysis of ATF, FBI, and DEA data

The next table shows rates of loss per month per 1,000 agents for the weapons and laptop computers that were lost, missing, or could not be categorized lost, stolen, or missing. ATF's rate of loss for those weapons (.28) was significantly higher than the FBI (.12) and DEA (.07). ATF's rate of loss for those laptop computers (2.53) was twelve times higher than the FBI (.21) and four times higher than the DEA (.63) rates of loss.

<sup>29</sup> To determine the losses reported per month per 1,000 agents, we first divided the number of total losses (76) by the number of months of the reporting period (59) to determine the number of losses per month. We then divided the losses per month by the number of total agents (2,461) to determine the number of losses per month per agent. Then we multiplied the number of losses per month per agent by 1,000, calculated as  $\{[(76 \div 59) \div 2,461] \times 1,000\}$ .

**LOST AND MISSING WEAPONS AND LAPTOP COMPUTERS  
PER MONTH PER 1,000 AGENTS - ATF, FBI and DEA<sup>30</sup>**

<b>LOST OR MISSING WEAPONS AND LAPTOP COMPUTERS</b>	<b>ATF</b>	<b>FBI</b>	<b>DEA</b>
<b>Number lost or missing weapons</b>	41	66	22
<b>Rate of Loss Per Month Per 1,000 Agents</b>	0.28	0.12	0.07
<b>Number of lost or missing laptop computers</b>	368	116	206
<b>Rate of Loss Per Month Per 1,000 Agents</b>	2.53	0.21	0.63

Source: OIG analysis of ATF, FBI, and DEA data

ATF officials were unable to explain why ATF's rates of loss were higher than those of the FBI and the DEA. While one official suggested that ATF agents may carry more weapons than FBI or DEA agents, we did not find support for this explanation.

We recognize that in an organization the size of ATF some weapons and laptop computers will inevitably be lost, stolen, or missing. However, it is important that ATF take appropriate steps to minimize these losses because they could damage ATF's operations, affect national security, or cause harm to persons whose personally identifiable information (PII) may have been compromised.<sup>31</sup> Moreover, we are concerned that ATF's rate of loss exceeds the rates in other DOJ law enforcement organizations.

When a weapon or laptop computer is lost, stolen, or missing, ATF must immediately report the loss, conduct an investigation, make any required entries into NCIC, and report the loss to DOJ. We discuss ATF's reporting and investigation of lost, stolen, or missing weapons in the next sections.

---

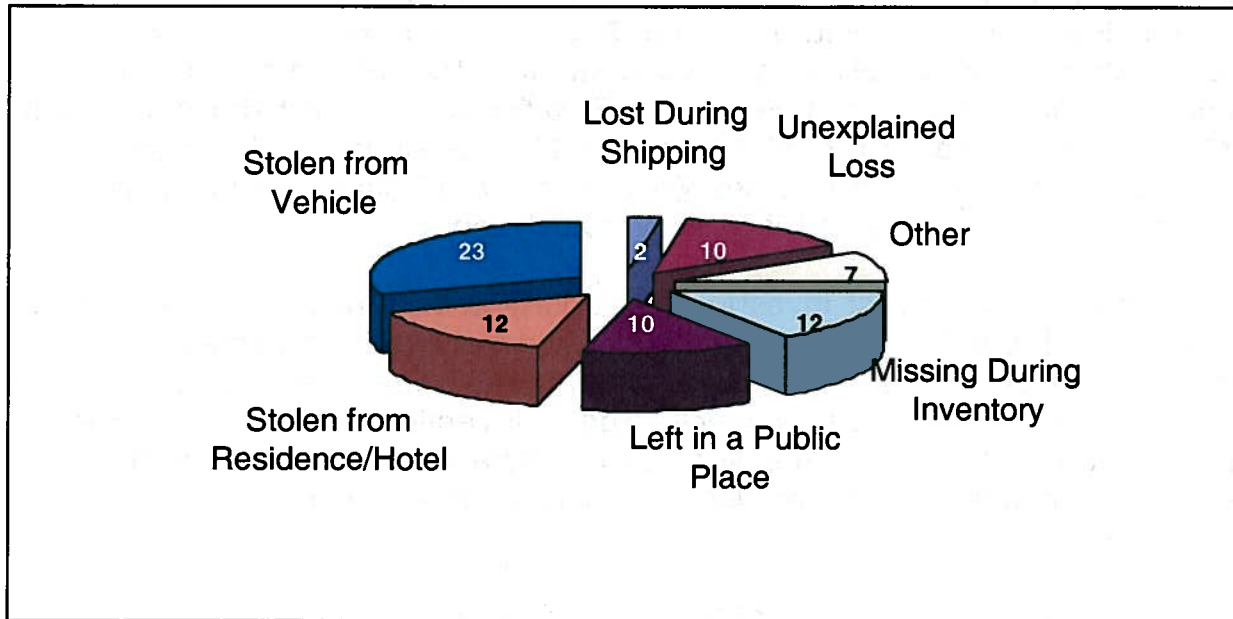
<sup>30</sup> Numbers in this table include weapons and laptop computers reported lost or missing and those that could not be categorized as lost, stolen, or missing. Statistics for the FBI and DEA also include weapons and laptop computers identified as missing during periodic inventories.

<sup>31</sup> According to OMB Memorandum M-07-16, dated May 22, 2007, PII 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 name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to an individual.

## Circumstances of Lost, Stolen, or Missing Weapons

We identified 76 lost, stolen, or missing weapons during our review period. Of these, 63 were reported to Internal Affairs and 13 were not. As shown in the following chart, these losses occurred under a variety of circumstances.

**NUMBER OF LOST, STOLEN, OR MISSING WEAPONS BY TYPE OF LOSS  
OCTOBER 1, 2002, THROUGH AUGUST 31, 2007<sup>32</sup>**



Source: OIG analysis of ATF Reports of Survey and investigative reports

Of the 35 stolen weapons, 23 were taken from government-owned or privately-owned vehicles and 12 were stolen from offices, residences, and hotel rooms.

Of the 41 lost weapons, 12 were identified by ATF staff as missing during an inventory, 10 were left in a public place, 2 were lost during shipping, 7 were reported as "other" losses, and 10 were unexplained. Other losses included a weapon that fell into the water while an agent was fishing and was never found. Unexplained losses are those not reported to Internal Affairs, and therefore documentation about the details of the losses was not available.

<sup>32</sup> The scope of our audit covered the 59-month period from October 1, 2002, through August 31, 2007. We asked ATF for documentation of all weapons and laptop computers identified as lost, stolen, or missing since October 1, 2002. ATF provided documentation for items lost, stolen, or missing from September 26, 2002, to July 24, 2007.

We reviewed the circumstances surrounding the loss of these firearms to determine whether the losses could have been prevented. In 23 of the 63 losses reported to Internal Affairs, thefts occurred despite ATF employees taking what appeared to be reasonable precautions. However, in 40 other instances the loss or theft of weapons appeared to result from employee carelessness or failure to follow ATF policy. For example, 10 losses occurred when agents left their weapons in public places such as in bathrooms (3), a dressing room (1), a shuttle bus (1), an airplane (1), a shopping cart (1), on a chair in a garage (1), and on the tops of vehicles as the employee drove off without the weapon (2). We were unable to determine whether carelessness was a factor in the remaining 13 lost, stolen, or missing weapons because ATF staff did not report those losses to Internal Affairs and documentation about 10 of those losses was not available. The other three losses were reported missing on Reports of Survey and were treated as inventory adjustments.

From our review of investigative reports at Internal Affairs, we learned that two stolen ATF weapons were recovered from suspects arrested for crimes. One weapon stolen from a government-owned vehicle parked at the Special Agent's home was recovered from a juvenile who used it to shoot out a window of a residence. Another weapon stolen from a cabinet in the Special Agent's laundry room was recovered from suspects arrested for burglaries.

In addition to the loss or theft of 76 ATF-owned weapons, ATF staff lost 3 seized weapons in 2 separate incidents. Two weapons were stolen from a government-owned vehicle in Macon, Georgia, and one was lost during Hurricane Rita. The details of each loss are discussed in Appendix III.

### **Circumstances of Lost, Stolen, or Missing Laptop Computers**

For the 59-month period covered by our audit, we identified 418 lost, stolen, or missing laptop computers. Of those 418, ATF identified 274 laptop computers as missing during an inventory. Documentation of inventory results submitted to ATF headquarters showed many of those laptop computers were kept in the property management records for several years before being deleted beginning in 2006. Officials from several ATF field offices said they believed that when laptop computers were replaced with newer models, exchanged because they were defective, donated to schools, or transferred to other ATF locations, documentation of these activities was not completed or the property records were not updated.

The eight laptop computers that were lost under other circumstances included three that were lost during shipping, one that was left on a train, one that was left on top of a car when the agent drove off, and one that was lost during a move to a new office location. Documentation about the remaining lost laptop computers did not fully explain the losses. The following table shows the lost, stolen, or missing laptop computers by loss type.

**LOST, STOLEN, OR MISSING LAPTOP COMPUTERS BY LOSS TYPE  
OCTOBER 1, 2002, THROUGH AUGUST 31, 2007**

<b>Total</b>	
<b>Lost:</b>	
Lost under various circumstances	8
<b>Subtotal</b>	<b>8</b>
<b>Stolen:</b>	
From a government-owned vehicle	12
From a personally-owned vehicle	7
From a rental vehicle	2
From an office	14
From a hotel room	4
From a residence	2
Other	3
Unexplained	6
<b>Subtotal</b>	<b>50</b>
<b>Missing:</b>	
Missing during inventory	274
<b>Subtotal</b>	<b>274</b>
<b>Could not categorize:</b>	
	86
<b>Subtotal</b>	<b>86</b>
<b>Total</b>	<b>418</b>

Source: OIG analysis of ATF Reports of Survey and investigative reports

Fifty laptop computers were stolen under various circumstances. In one incident, six laptop computers were stolen from an ATF office in Philadelphia but were recovered a week later. In another incident, five laptop computers were stolen from an ATF office in Houston. Another laptop

was stolen from a room at the Cardozo School of Law in New York during a law school competition where an ATF employee was a judge. One laptop was believed to have been taken by an employee when the employee transferred to a new duty station. The employee's supervisor referred the matter to Internal Affairs, which found no wrongdoing. Six other laptop computers were identified as stolen, but the available documentation provided no details about the nature of the thefts.

For 86 laptop computers, we could not determine whether the losses should be categorized as lost, stolen, or missing because ATF could not provide documentation used to remove those items from the property records. This occurred because ATF only retained those documents for the current year and 2 prior years.

### **Reporting Weapon and Laptop Computer Losses**

ATF policy states that when a weapon or laptop computer is lost, stolen, or missing, the loss should immediately be reported to the Special Agent in Charge, division director, or chief who, in turn, must report the loss to the property accountable officer within 10 days. The property accountable officer, who is responsible for removing items from active property list, should then prepare a Report of Survey and provide a copy with any other documentation to Internal Affairs. However, during our review of the incident reports at Internal Affairs, we generally found that the Special Agent in Charge, division director, or chief notified Internal Affairs directly rather than submitting the incident report to the property accountable officer. When a loss is reported directly to Internal Affairs, the property accountable officer may not be aware of the loss and therefore not remove it from the property records. In addition, the property accountable officer does not have an opportunity to review the report to ensure that Internal Affairs receives complete information and documentation.<sup>33</sup> Findings of an Internal Affairs investigation are referred to a Professional Review Board for adjudication, as described in this report under "Referring and Investigating Losses."

ATF's written policy does not contain procedures to assess the contents of a lost, stolen, or missing laptop computer, whether or not the

---

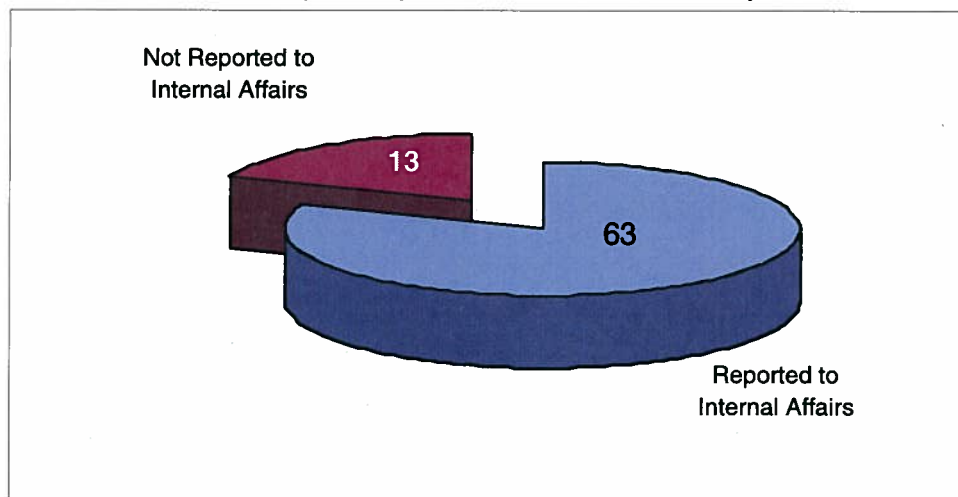
<sup>33</sup> On April 29, 2008, ATF issued a new property management policy that allows the SAC, division director, or chief to report losses directly to Internal Affairs. However, ATF's new policy does not ensure that such losses are also reported to the property accountable officer so that the property can be removed from the property records to maintain an accurate inventory.

laptop computer contained sensitive or classified information, or whether the loss compromised sensitive or National Security Information. An ATF Information Systems Security Officer told us that ATF Office of Science and Technology staff interviews personnel to determine what information was on the lost, stolen, or missing laptop computers, such as dates of birth, addresses, phone numbers, social security numbers (SSN), and investigative case information. However, we believe ATF needs to develop written procedures to identify the contents of lost, stolen, or missing laptop computers in order to reduce the possibility that the loss of sensitive or classified information could damage ATF operations or national security.

### *Weapons*

We tested whether the 76 lost, stolen, or missing weapons were reported to Internal Affairs. As shown in the following chart, 63 (83 percent) of the 76 weapons were referred to Internal Affairs.

#### **LOST, STOLEN, OR MISSING WEAPONS REPORTED TO INTERNAL AFFAIRS OCTOBER 1, 2002, THROUGH AUGUST 31, 2007**



Source: OIG analysis of ATF data

Of the 76 lost, stolen, or missing weapons, 13 (17 percent) were not reported to Internal Affairs for follow-up actions even though such referral is required by ATF policy. ATF provided documentation showing these items were removed from the property records using a Report of Survey, but could not explain why the items were not reported to Internal Affairs. Unless such losses are reported to Internal Affairs and an investigation into the loss is conducted, ATF may never know the facts surrounding the loss and appropriate disciplinary action may not be considered.

The analyses found later in this report concerning the timeliness of reporting and the actions taken in response to the reports are limited to the 63 weapons that were reported to Internal Affairs.

### *Laptop Computers*

Although ATF policy requires that all lost, stolen, or missing laptop computers be reported to Internal Affairs, the policy does not require a Professional Review Board to become involved in each loss.<sup>34</sup> An Internal Affairs official told us that few laptop computer losses are investigated because only losses that result from failure to follow an established policy or from employee misconduct will result in any disciplinary action. ATF Policy 7500.1 provides mandatory and preferred methods of security for protecting laptop computers while they are in the office and during travel.

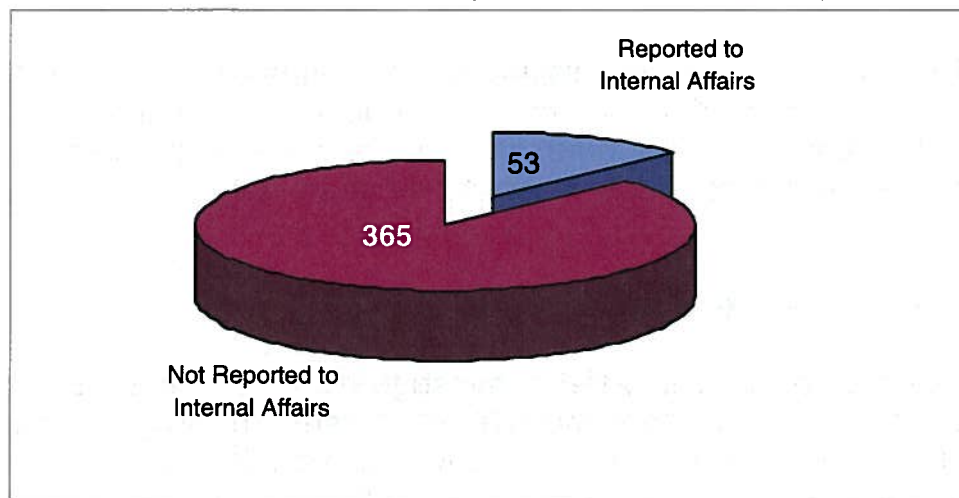
Only 53 lost, stolen, or missing laptop computers (13 percent) were reported to internal Affairs, as shown in the following table.

---

<sup>34</sup> JMD policy states that inventory discrepancies do not need to be referred to a Board of Survey. ATF categorized many laptop computer losses as inventory discrepancies, but ATF could not provide documentation confirming that the losses were only inventory discrepancies and not laptop computers that were identified as missing during an inventory.



**LOST, STOLEN, OR MISSING LAPTOP COMPUTERS REPORTED TO INTERNAL AFFAIRS OCTOBER 1, 2002, THROUGH AUGUST 31, 2007**



Source: OIG analysis of ATF data

The analyses that follow concerning timeliness of reporting and actions taken based on the reports are limited to the 53 that were reported to Internal Affairs.

*Timeliness of Loss Reporting*

To determine whether ATF staff immediately reported the loss or theft of their weapons or laptop computers to a supervisor such as a SAC, division director, or chief, we reviewed documentation maintained by the Office of Internal Affairs.<sup>35</sup>

We found that ATF staff reported 57 of 63 lost, stolen, or missing weapons to Internal Affairs, within 1 day or less from when the loss occurred. Four lost, stolen, or missing weapons were reported from 2 to 19 days after the loss occurred. In one of those cases, an agent did not report the loss of a weapon at all. Instead, 19 days after the loss occurred, a local police department issued a trace on the weapon and notified the agent's supervisor. ATF staff could not explain why the other three losses were not reported immediately, but an Internal Affairs manager told us all employees who did not immediately report the loss of their weapons were suspended without pay and that all the lost, stolen, or missing weapons were the agents' backup weapons. We could not determine whether the

---

<sup>35</sup> ATF did not define that term "immediately." We defined "immediately" as 1 day or less. Any item reported after 1 day would not be considered as having been reported immediately.

remaining two losses were reported timely because the exact loss date was unclear.

Of the 53 lost, stolen, or missing laptop computers reported to Internal Affairs, ATF staff reported 46 within 1 day or less from when the loss occurred. We could not determine whether the remaining seven laptop computers were reported timely because we could not determine the exact loss date.

## **Investigations and Consequences of Losses**

ATF's Office of Internal Affairs investigates, tracks, and reports allegations of misconduct involving ATF employees. In property loss cases, Internal Affairs conducts a preliminary investigation to determine whether employee actions or behavior caused a loss of property or violated ATF policies. Depending on the results, the preliminary investigation can be closed or converted to a full internal investigation. An ATF Professional Review Board adjudicates the results of any internal investigation and a headquarters-level deciding official makes a final decision on any disciplinary actions proposed by the Professional Review Board.

An Internal Affairs official told us that each reported loss of a weapon or laptop computer is assigned to an Internal Affairs agent to investigate. Upon completion of the investigation, the Internal Affairs agent prepares a Report of Investigation and provides a copy to the Internal Affairs SAC or Assistant SAC.

Disciplinary actions that can result from property losses include receiving a Letter of Caution, reprimand, suspension of from 1 to 10 days, or termination.<sup>36</sup> Employees may also receive a Memorandum of Clearance showing they have been cleared of any wrongdoing. For the cases we reviewed, the disciplinary actions taken depended on the nature of the incident and whether the case involved a failure to properly secure or store a weapon.

The following table summarizes the numbers of lost, stolen, or missing weapons and laptop computers referred to and investigated by the Office of Internal Affairs.

---

<sup>36</sup> ATF officials did not consider a Letter of Caution as a disciplinary action; however, we included it in our report as a form of discipline.

**LOST, STOLEN, OR MISSING WEAPONS AND LAPTOP COMPUTERS  
REPORTED TO AND INVESTIGATED BY INTERNAL AFFAIRS**

<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
<b>Category</b>	<b>Number Lost, Stolen, or Missing</b>	<b>Number Reported to Internal Affairs</b>	<b>Number Investigated by Internal Affairs</b>	<b>Number Not Investigated by Internal Affairs</b>
Lost Weapons	41	28	28	13
Stolen Weapons	35	35	35	0
<b>Total Lost, Stolen, or Missing Weapons</b>	<b>76</b>	<b>63</b>	<b>63</b>	<b>13</b>
Lost Laptop Computers	368	9	9	359
Stolen Laptop Computers	50	44	44	6
<b>Total Lost, Stolen, or Missing Laptop Computers</b>	<b>418</b>	<b>53</b>	<b>53</b>	<b>365</b>

Source: OIG analysis of ATF data

*Weapons Losses*

As shown in the preceding table, 63 (83 percent) of 76 lost, stolen, or missing weapons were referred to and investigated by ATF's Office of Internal Affairs. Of the 63 lost, stolen, or missing weapons were reported to the Office of Internal Affairs:

- 32 resulted in the employees being suspended for 1 to 10 days;
- 6 had disciplinary action still pending with the Professional Review Board as of March 2008;
- 6 resulted in the employees receiving a Letter of Caution;
- 1 resulted in the employee receiving a reprimand; and
- 1 resulted in the employee being terminated;
- 6 resulted in the employees receiving a Memorandum of Clearance; and
- 11 were closed after a preliminary investigation found no employee wrongdoing.

Based on our review of each of these cases, we did not identify any overt inconsistencies in disciplinary actions.

Prior to June 2007, most ATF employees received a 3-day suspension without pay for the first-time loss of a weapon. However, in June 2007 ATF changed the penalty for the first-time loss of a weapon from a minimum 3-day suspension to a minimum 1-day suspension. An ATF official told us the agency changed the policy because a minimum 3-day suspension for the loss of a weapon, regardless of the circumstances, might deter prompt reporting of the loss. Reducing the penalty to a 1-day suspension, the official said, would motivate the agent to report the loss quickly so that the lost, stolen, or missing item could be entered into NCIC. Some cases resulted in no disciplinary actions because ATF concluded there was no employee misconduct. One case resulted in termination because the employee had also misused his government-issued credit card and vehicle.

Some personnel received suspensions of more than 3 days because they had been involved in prior losses of weapons or the nature of the loss included other circumstances, such as not reporting the loss to a supervisor. For example, one agent received a 10-day suspension for the second loss of his weapon within a 1-year period. In another case, an agent who received a 10-day suspension had also received a 2-day suspension in 2002 for losing a weapon and a reprimand in 2003 for misuse of his official credentials. In a third case, an employee received an 8-day suspension because he did not report the loss of his weapon. Instead, a local police department issued a trace on the weapon and notified the ATF.

### *Laptop Computer Losses*

As shown in the preceding table, Internal Affairs conducted a preliminary investigation into all 53 of the reported lost, stolen, or missing laptop computers, and opened a full investigation into 6 (11 percent) of the losses. Internal Affairs staff told us that full investigations were not conducted for the remaining 47 losses reported because the preliminary investigations found no employee misconduct. Of the six laptop computer losses that were fully investigated:

- 3 resulted in the employee receiving a written reprimand,
- 1 resulted in the employee receiving a Memorandum of Clearance, and
- 2 resulted in no documented disciplinary action.

Because ATF did not refer the remaining 365 lost, stolen, or missing laptop computers to Internal Affairs for investigation, ATF will never know

the facts surrounding the losses or how to prevent their reoccurrence, and employees responsible for the losses may not receive appropriate disciplinary action.

### **Contents of Lost, Stolen, or Missing Laptop Computers**

Beginning in November 2003, DOJ required all components to respond to and report all computer security incidents, including those that result in the loss or compromise of information, to the Department of Justice Computer Emergency Readiness Team (DOJCERT). DOJCERT is a centralized incident response team that provides Department-wide support for computer security incidents 24 hours a day, 7 days a week. DOJCERT is discussed in more detail in Finding II of this report.

In May 2006, OMB required all Department components to review their policies to ensure they had adequate safeguards in place to protect PII and to remind employees of their responsibilities for protecting such information. In May 2007, OMB required all departments and agencies to develop and implement a plan to notify persons whose PII had been compromised.

At the time of our audit, ATF did not have written procedures to determine whether lost, stolen, or missing laptop computers contained sensitive or classified information. However, an ATF Information Systems Security Officer (ISSO) told us ATF has an unwritten policy that when a user reports the loss or theft of a laptop computer, the ATF Helpdesk or the ISSO interviews the user about the contents of the laptop computer and enters the results of those interviews into the DOJCERT incident response database. In addition, Internal Affairs reports sometimes contained information about the contents of lost, stolen, or missing laptop computers.

We believe that a clear policy requiring ATF personnel to determine the contents of lost, stolen, or missing laptop computers is critical. Without knowing the contents, ATF does not know the extent of the damage these losses might have on operations, individual security, or national security.

On March 12, 2007, in response to the theft of two laptop computers, ATF's Chief Information Officer issued a memorandum to all ATF employees explaining the importance of safeguarding laptop computers. He wrote that regardless of a thief's intent, if sensitive information from a stolen laptop computer was accessed by the thief, the consequences could be serious. The memorandum reminded employees they should immediately report computer security incidents to the Help Desk and if the laptop computer were stolen they should also submit a Theft of Government Property report

to an immediate supervisor. However, this policy still does not require ATF to determine whether lost, stolen, or missing laptop computers contained sensitive or classified information.

### *Unknown Contents for 398 Laptop Computer Losses*

To determine whether sensitive information, including PII or classified information, may have been stored on the lost, stolen, or missing laptop computers, we interviewed ATF staff, reviewed Internal Affairs reports, and reviewed documentation of incidents ATF reported to DOJCERT. As explained earlier, interviews to determine the contents of lost, stolen, or missing laptop computers may also be documented on reports submitted to DOJCERT. We therefore asked ATF staff to provide incident reports submitted to DOJCERT and ATF Internal Affairs reports on all 53 lost, stolen, or missing laptop computers reported to Internal Affairs. ATF provided all 53 Internal Affairs reports we requested. However, it provided DOJCERT reports for only 6 (11 percent) of the 53 laptop computers.<sup>37</sup>

Of the 20 laptop computers for which ATF staff provided documentation, 7 reports indicated that the laptop computers contained sensitive information. None of the documents we reviewed indicated those stolen laptop computers contained classified information.

ATF staff could not provide documentation showing whether the remaining 398 lost, stolen, or missing laptop computers contained sensitive or classified information. We asked an official whether ATF was able to determine the contents of these laptop computers, but, as of July 2008, we had not received a response.

Unless ATF knows the contents of lost, stolen, or missing laptop computers, it cannot assess what damage those losses could have on operations, national security, or on individuals whose personal information may have been compromised. Details of sensitive information contained on the 7 stolen laptop computers are shown in the following table.

---

<sup>37</sup> ATF provided DOJCERT reports for nine other lost, stolen, or missing laptop computers. Four of those were lost, stolen, or missing during the period covered by our audit and five were lost, stolen, or missing after the period covered by our audit.

**STOLEN LAPTOP COMPUTERS THAT CONTAINED SENSITIVE INFORMATION**

<b>No.</b>	<b>Source</b>	<b>Date of Loss</b>	<b>Office Reporting Loss</b>	<b>Encrypted<sup>38</sup></b>	<b>Nature of Contents</b>
1	Internal Affairs Report	6/25/2005	Washington Field Division	No	Sensitive but unclassified information but did not specify the type of data.
2	Internal Affairs Report	4/2/2006	Los Angeles Field Division	No	Explosives licensee information.
3	Internal Affairs Report	9/28/2006	Detroit Field Division	No	Personal and work-related information.
4	Internal Affairs Report	11/1/2006	Office of Science and Technology	No	Employee evaluations, including social security numbers and other PII.
5	Internal Affairs Report and DOJCERT Report	2/27/2007	Financial Investigations Service Division	No	Approximately 300-500 names with dates of birth and social security numbers of targets of criminal investigations including their bank records with financial transactions.
6	Internal Affairs Report and DOJCERT Report	2/27/2007	Financial Investigations Service Division	No	Active case information, PII of ATF personnel, and copies of administrative reports.
7	Internal Affairs Report	6/9/2007	Computer Forensics Branch	Could Not Determine	Names and addresses of ATF computer forensic examiners.

Source: ATF incident reports and investigative reports

According to Internal Affairs records, ATF conducted a full internal investigation into only one of the laptop computer losses known to contain sensitive information (item 2 in the preceding table, containing explosives licensee information). ATF did not take any disciplinary action against the employees assigned any of these stolen laptop computers. An Internal Affairs manager told us only those losses that result from failure to follow an established policy or from employee misconduct result in any disciplinary action.

We believe that ATF management should strengthen its controls to ensure that ATF responds appropriately to each laptop computer loss. This includes determining the contents of lost laptop computers through

---

<sup>38</sup> Laptop computers lost, stolen, or missing prior to May 2007 did not have encryption software installed.

interviewing employees or maintenance of inventories of information stored on laptop computers. However, because ATF has no written policy to obtain such information, it relies on users to voluntarily provide an inventory of the contents of the lost, stolen, or missing computer.

The previously mentioned memorandum regarding laptop computers, dated March 12, 2007, was a step in improving ATF's policy because it established written guidelines to protect data and laptop computers. However, it did not require the ATF to determine the contents of lost, stolen, or missing laptop computers. The lack of a policy requiring determination of information on laptop computers is a significant deficiency because ATF laptop computers may contain sensitive information, such as PII or investigative case files.

In our audit, we sought to identify the types of information generally stored on ATF laptop computers by meeting with 16 Special Agents, 1 supervisory Special Agent, 2 contractors, 2 Task Force Officers and 2 other ATF employees in the ATF Atlanta area offices in March 2008. We interviewed those individuals about the contents of their laptop computers and found the hard-drives contained sensitive information such as names, addresses, SSNs, investigative case file information, and employees' personal information. The sensitive information included:

- travel voucher claim forms containing Special Agents' names and SSNs;
- a list of about 20 websites with the user's logon and password information;
- a fingerprint request form containing an arrestee's name, date of birth, SSN, and date of arrest;
- a document containing a fugitive's name, SSN, biometric information, last known address, phone number, and relatives' names;
- reports containing suspects' names, addresses, SSNs, and dates of birth;
- recordings of phone conversations with targets of investigations;
- emergency data sheets with Special Agents' and their family members' names, home addresses, SSNs, and dates of birth; and



- ATF vehicle license-plate numbers and the names of the Special Agents' to whom those vehicles were assigned.

Because ATF laptop computers contained these types of sensitive information, we believe that the lack of controls for determining the contents of lost, stolen, or missing laptop computer is a significant deficiency.

In addition, ATF should ensure laptop computers are encrypted. Although encryption does not negate the need to determine the contents of lost, stolen, or missing laptop computers, it reduces the likelihood the information will be misused. We discuss encryption in detail in Finding II.

### **Entering Losses into NCIC**

ATF Memorandum 3120, dated March 26, 2002, requires ATF employees to enter all lost, stolen, or missing weapons into NCIC. Although the memorandum did not require ATF to enter laptop computers into NCIC, we found that some lost, stolen, or missing ATF laptop computers were entered into NCIC anyway.

On April 29, 2008, ATF issued a revised property management policy, ATF Order 1850.2D, requiring that lost, stolen, or missing firearms or equipment containing classified information should be reported to NCIC. However, the new property management policy still does not require all lost, stolen, or missing laptop computers to be reported to NCIC.<sup>39</sup>

We tested whether 72 of 76 lost, stolen, or missing weapons were entered into NCIC. We could not test the four remaining losses. We found that 7 of the 72 did not need an NCIC entry because the weapons were recovered shortly after being reported lost or stolen. Of the remaining 65, lost, stolen, or missing weapons tested, 60 (92 percent) had an NCIC record and 5 did not. Specifically, we found that:

- 45 had an active record in the NCIC database,
- 15 had an NCIC record at one time but the weapons were recovered and the records were purged from NCIC,

---

<sup>39</sup> Although DOJ policy does not require that lost, stolen, or missing laptop computers be entered into NCIC, FBI and DEA have policies that require that such laptop computers be entered into NCIC.

- 5 did not have an NCIC record. As of July 2008, ATF staff had not responded to our inquiry about why these records had not been reported to NCIC.

We also tested whether all 53 of the lost, stolen, or missing laptop computers reported to Internal Affairs were entered into NCIC. We found that 29 (55 percent) of 53 lost, stolen, or missing laptop computers we tested were entered into NCIC. In addition, we found that:

- 11 had an active record in the NCIC database;
- 18 had an NCIC record at one time but the laptop computers were recovered and the records were purged from NCIC;
- 4 were not applicable because they were mistakenly identified as lost, stolen, or missing or were recovered shortly after they were lost, stolen, or missing; and
- 20 did not have an NCIC record. Neither DOJ nor ATF had a policy requiring ATF to enter lost, stolen, or missing laptop computers into NCIC.

An ATF Office of Strategic Intelligence and Information official told us that when a weapon or laptop computer is reported lost, stolen, or missing at the agent's residence, the loss is to be reported to the local law enforcement agency and the local law enforcement agency enters the loss into NCIC; otherwise, ATF enters the losses in NCIC. When an item is subsequently located by local law enforcement, the local agency flags the NCIC record to indicate the item has been located and then notifies ATF staff who remove the NCIC record entry. If ATF does not remove the record within 10 days, the flag entered by the locating agency causes the record to automatically be deleted from the system. Although ATF Order 1850.2D required that all lost, stolen, or missing firearms and equipment containing classified information be reported to NCIC, in our opinion the new property management policy falls short because it does not require that all lost, stolen, or missing laptop computers be reported. FBI and DEA policies require that lost, stolen, or missing laptop computers be entered into NCIC. A lost, stolen, or missing ATF laptop may have extremely sensitive case-related or operational information that could be damaging if accessed by non-ATF personnel.

## **Ammunition and Explosives Losses**

ATF has a policy for reporting the loss of explosives, but did not have a specific written policy for reporting the loss of ammunition during our audit period. ATF's property management policy requires employees to report losses of government property assigned to them. An ATF official told us that the policy covers losses of ammunition, which was specifically included in a revision issued in April 2008. However, the policy in place at the time of our audit did not specifically include ammunition and stated that a record is established within the property management system for each property asset, and ammunition is not included in the system. Therefore, it appears that ammunition was not property covered by the property management policy during our audit period.

An ATF Internal Affairs manager also told us that individual circumstances, such as whether the ammunition was stolen in conjunction with a stolen weapon, dictate whether lost, stolen, or missing ammunition should be referred to Internal Affairs and whether Internal Affairs conducts a full internal investigation into the loss. Because expendable items such as ammunition and explosives are not included in ATF's property management system, we could only identify losses that ATF staff reported to Internal Affairs.

Although expendable items such as ammunition and explosives are not included in ATF's electronic property management system, ATF accounts for those items using a paper-based perpetual recordkeeping system.<sup>40</sup> Internal controls for ammunition and explosives are discussed later in Finding III of this report. Because these items are not included in the electronic property management system, we could only identify losses that ATF staff reported to Internal Affairs.

### *Ammunition*

ATF staff reported to Internal Affairs 12 instances of lost, stolen, or missing ammunition for the 59-month period, October 1, 2002, through August 31, 2007. The 12 losses are detailed in the following table.

---

<sup>40</sup> Expendable property is property used for consumption.

### AMMUNITION LOSSES REPORTED TO INTERNAL AFFAIRS

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS
1	7/8/2003	Lexington, Kentucky	24 rounds of .40 caliber and 2 ammunition magazines were stolen from an ATF vehicle parked at a residence. <sup>41</sup>
2	3/21/2004	Lubbock, Texas	An unknown amount of ammunition was stolen from an ATF storage shed at the Lubbock Police Department's firing range.
3	7/14/2004	New Haven, Connecticut	18 boxes (360 rounds) of .40 caliber ammunition were stolen from a government-owned vehicle parked in a residence driveway. ATF later recovered 112 rounds.
4	6/30/2005	Tulsa, Oklahoma	A partial case of .40 caliber, a partial case .40 caliber frangible, and 1 case of .223 caliber frangible were stolen from a government-owned vehicle parked at a hotel. <sup>42</sup> (This incident included a weapon loss that we included in our weapon loss review.)
5	8/2/2005	San Antonio, Texas	3 magazines of .40 caliber ammo and 60 rounds of .40 caliber ammunition were stolen from a government-owned vehicle parked at a hotel.
6	1/15/2005	Honolulu, Hawaii	39 rounds of ammunition were stolen from an ATF vehicle parked at a residence. The Special Agent received a Letter of Caution.
7	3/1/2006	Detroit, Michigan	2 cases of .40 caliber were found missing during an inventory. After a division-wide e-mail requesting return of the missing ammo, one case was anonymously returned. Another was discovered lodged between two of the pallets of ammunition. <sup>43</sup>
8	5/2/2006	New York, New York	15-20 rounds of .40 caliber ammunition were stolen from a government-owned vehicle. Damage to trunk lock.
9	6/9/2006	Computer Forensics Branch	24 rounds of .40 caliber missing.
10	Unknown	Colorado Springs, Colorado	1 box miscellaneous ammunition was stolen from a government-owned vehicle.
11	Unknown	Wilmington, Delaware	5 rounds of .22 caliber. Ammunition was stored in an unsealed envelope and must have fallen out of the envelope sometime during a move.

<sup>41</sup> An ammunition magazine is a compartment in the weapon, or a small box that can be attached to the weapon, which holds ammunition to be fed into the firing chamber of the weapon. An explosives storage magazine is usually several feet tall and wide.

<sup>42</sup> Frangible rounds are designed to break apart when they hit walls or other hard surfaces to prevent ricochets during close-quarters combat.

<sup>43</sup> A pallet is a portable platform for storing or moving goods that are stacked on it. See a photo of a pallet in Finding III, Ammunition Controls section.

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS
12	Unknown	New Orleans, Louisiana	A .40 caliber magazine with ammunition was stolen from a government-owned vehicle.

Source: ATF incident reports and investigative reports

Of the 12 incidents of lost, stolen, or missing ammunition, 1 resulted in the employee being cleared of misconduct. This incident also included an investigation of a stolen weapon discussed previously. One other ammunition loss resulted in the agent receiving a Letter of Caution. There was no report of investigation or disciplinary action for the remaining 10 incidents. Because ATF did not have specific written policies for reporting losses of ammunition to Internal Affairs it is possible that not all losses were reported for investigation, and therefore would not have been included in this review. The previous Treasury audit did not identify any reported ammunition losses.

### *Explosives*

ATF staff reported to Internal Affairs two instances of lost, stolen, or missing explosives during our review period. The two losses are detailed in the following table.

#### **EXPLOSIVES LOSSES REPORTED TO INTERNAL AFFAIRS**

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS
1	2/27/2003	Fort A.P. Hill, Virginia	Inert improvised explosives device stolen from camper shell of an ATF vehicle and later recovered at Fredericksburg, VA.
2	Unknown	Kansas City, Missouri	Three canine training explosives (10 grams each) were discovered missing. The explosives were found in the explosives storage unit several weeks later.

Source: ATF incident reports and investigative reports

ATF opened preliminary investigations into both incidents but found no misconduct and imposed no discipline. In both cases the explosives were either recovered or later found in the explosives storage unit. The previous Treasury audit did not identify any reported explosives losses.

### **Conclusion**

Since the Treasury OIG's 2002 audit, the number of lost, stolen, or missing weapons has increased from 0.47 per month to 1.29 per month. On

an agent-per-month basis, this rate of loss is nearly double the rate of loss for the FBI and DEA. In addition, the numbers of lost, stolen, or missing laptop computers also increased dramatically since the 2002 audit. On a monthly basis, ATF's rate of loss has dramatically increased.

ATF reported 82 percent of lost, stolen, or missing weapons and few of the lost, stolen, or missing laptop computers to Internal Affairs for follow-up actions. ATF officials did not explain why staff did not report 13 lost, stolen, or missing weapons. ATF officials told us they do not report inventory discrepancies as missing property to Internal Affairs. That decision is consistent with DOJ policy. Of the remaining 144 laptop computers, 53 (37 percent) were reported to Internal Affairs. ATF did not explain why staff did not report 91 lost, stolen, or missing laptop computers to Internal Affairs for follow-up action.

Internal Affairs opened a full internal investigation into only 6 of 53 laptop computers reported as lost, stolen, or missing. An Internal Affairs official told us ATF did not conduct an internal investigation or discipline employees for the other 47 losses because a preliminary investigation found no employee misconduct.

We determined that 92 percent of all lost, stolen, or missing weapons we tested were entered into NCIC. Although ATF was not required to enter lost, stolen, or missing laptop computers into NCIC, 55 percent of those we tested were entered anyway. We learned from our review of Internal Affairs documents that two stolen weapons subsequently were used in the commission of a crime.

ATF did not have written policies for determining the contents of lost, stolen, or missing laptop computers. ATF officials told us that when a laptop computer is lost, stolen, or missing, staff from the Help Desk or Internal Affairs or an Information Systems Security Officer interview the user of the laptop computer to determine its contents and that the results of those interviews are documented on Internal Affairs and DOJCERT reports. However, for most lost, stolen, or missing laptop computers, ATF could not provide documentation showing whether those laptop computers contained sensitive or classified information.

An ATF memorandum, dated March 12, 2007, improved ATF's controls over laptop computers because it established written guidelines to protect data, but it did not require ATF to determine the contents of lost, stolen, or missing laptop computers.

## **Recommendations**

We recommend that ATF:

1. Ensure that ATF staff notify the Materiel Management Branch of all weapon and laptop computer losses and maintain copies of all supporting documentation.
2. Ensure that for each loss Materiel Management provides Internal Affairs with the Report of Survey and information needed to conduct an investigation.
3. Implement a written policy for reporting losses of ammunition to Internal Affairs for investigation.
4. Implement procedures to determine the contents of lost, stolen, or missing laptop computers, specifically:
  - a. whether the laptop computer contained classified information;
  - b. whether the laptop computer contained sensitive or personally identifiable information; and
  - c. whether the lost, stolen, or missing laptop computer was protected with encryption software.
5. Require that lost, stolen, or missing weapons and laptop computers are appropriately entered into NCIC.

## **II. INTERNAL CONTROLS OVER WEAPONS AND LAPTOP COMPUTERS**

ATF did not maintain accurate and complete records in its property management system to track weapons and laptop computers and did not update the system to reflect the results of its inventories. Further, ATF did not submit semiannual loss reports identifying weapon and laptop computer losses to DOJ and laptop losses to DOJCERT as required. Additionally, ATF did not maintain support documentation for 5 disposed weapons and 22 disposed laptop computers tested and did not ensure that hard drives for 112 laptop computers were cleared prior to disposal.

### **Physical Inventories**

DOJ Property Management Regulations require all components to conduct an annual physical inventory of all non-expendable personal property.<sup>44</sup> However, at the discretion of the component head, these inventories can be conducted every 2 years rather than annually. ATF Order 3020.1 requires annual inventories of weapons. ATF performed annual inventories of weapons and bi-annual inventories of laptop computers recorded in its automated property system.

We reviewed ATF-wide inventory reports for FYs 2006 and 2007. The reports identified adjustments to the property records based on physical inventories performed. Not all divisions were listed on the ATF-wide consolidated report, so not all divisions had adjustments. We also reviewed inventory reports at the field divisions we tested. The divisions provided these reports, which include property overages and shortages, to the ATF property accountable officer. ATF policy required the property accountable officer to reconcile the shortages, post any administrative changes to the property management system, and prepare Reports of Survey for items that ATF could not reconcile.

We found that ATF property accountable officers did not consistently post changes to the property management system based on inventory results from the divisions. As a result, ATF kept many items on the active property list when it no longer had the property. This included items that were properly disposed of, as well as lost, stolen, or missing items. In one case, property was removed from the active property inventory 4 years after

---

<sup>44</sup> DOJ Property Management Regulations cover personal and real property.



the item was first reported missing.<sup>45</sup> By not timely updating the property management system based on results of annual inventories, ATF diminished its ability to maintain an accurate inventory of its weapons and laptop computers.

### **Reconciling Property Records to the Financial System**

ATF's financial system is not integrated with its property management system and the two systems are not reconciled. We performed tests to determine whether weapons and laptop computer purchases recorded in the financial system were recorded in the property management system.

We judgmentally selected from the financial system four purchases of weapons from April 7, 2000, through September 24, 2007. The purchases were for 1,264 weapons valued at \$737,133. We found no discrepancies when we traced all the purchases to ensure that the items purchased were entered into the property management system.

ATF had no laptop computer procurement records to test because ATF did not enter these items into its financial system. Rather, ATF leased laptop computers from a contractor and the contractor used a software program to track the laptop computers ATF used.<sup>46</sup> Once a month, the software scanned the ATF network to identify all laptop computers connected to the network during the previous 90 days and the contractor billed the ATF for those laptop computers. Because ATF leased laptop computers and was billed monthly, the agency had no laptop computer procurement records to test. Therefore, we were unable to determine the adequacy of ATF's controls for reconciling laptop computer property records to the financial system because the leased computers were not entered into the financial system.

After the laptop computers are replaced by new leased laptop computers, most of the replaced laptop computers were disposed of. This represents a refresh cycle of 3 years that is normal in the computer industry. At the end of the refresh period, ATF owned the replaced computers and maintained a few of them for special purposes.

---

<sup>45</sup> ATF requires that a loss be reported to the Materiel Management Branch within 10 days after the loss is identified.

<sup>46</sup> The monthly lease amount was \$310, which includes \$77 for the laptop and \$233 for support services such as managing the server and providing data security and round-the-clock technical support.

## **Inaccurate and Incomplete Property Records**

We found inaccurate and incomplete data in ATF's property management system that tracks its weapons and laptop computers. We tested weapons and laptop computers in two phases. First, we completed a 100-percent inventory of weapons and laptop computers at two field divisions. Based on the results of those tests, we performed a second phase of testing during which we selected a statistical sampling of weapons and laptop computers from the property management system and attempted to verify the information.

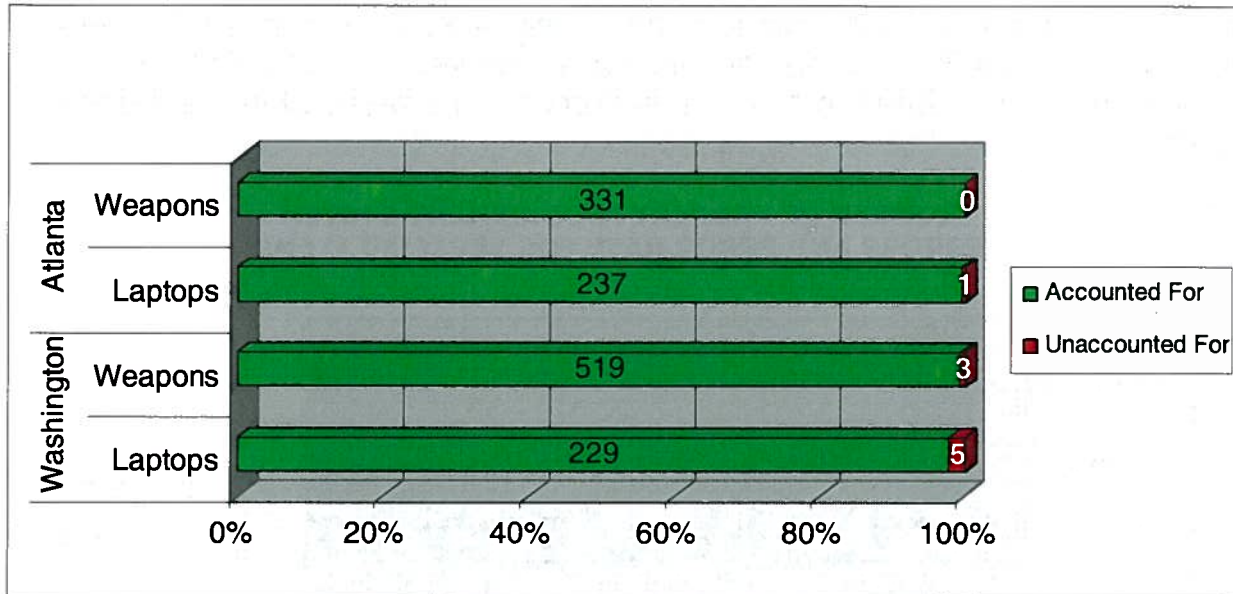
### *Preliminary Audit Testing (Phase I)*

During this phase, we selected the Atlanta and Washington Field Divisions to examine the accuracy and completeness of property records in the property management system.<sup>47</sup> We identified all weapons and laptop computers in the property management system for both divisions and completed a 100-percent review by verifying the existence of the property either by physically inspecting the equipment or by confirmation memoranda. We also evaluated property records and property management activities. The results of the review are shown in the following chart.

---

<sup>47</sup> The Atlanta Field Division includes field offices in Georgia that include Atlanta, Macon, Savannah, Columbus, and Augusta. The Washington Field Division includes field offices in Washington, D.C., Virginia, and West Virginia. The Virginia offices include Falls Church, Richmond, Roanoke, Charlottesville, Norfolk, Bristol, and Winchester. West Virginia has a single field office in Martinsburg.

**TOTAL ITEMS TESTED**



Source: OIG verification and analysis of ATF property management system data

The items we did not account for were not physically present during our review and the division did not respond to a request for property confirmation memoranda.<sup>48</sup> We consider these three weapons and six laptop computers to be unaccounted for.

For the items we did verify, we either physically verified the item or verified the item by confirmation memoranda. We detail the method of verification in the following table.

**TOTAL VERIFIED ITEMS**

Verification Method	Field Division			
	Atlanta		Washington	
	Weapons	Laptops	Weapons	Laptops
Physically Verified	280	210	462	189
Verified by Confirmation Memoranda	51	27	57	40
<b>TOTALS</b>	<b>331</b>	<b>237</b>	<b>519</b>	<b>229</b>

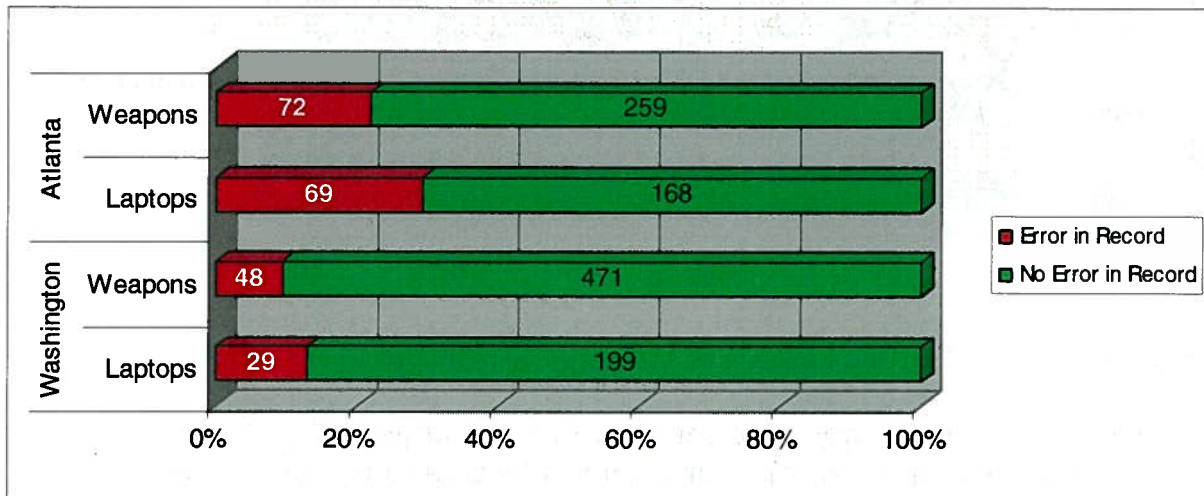
Source: OIG verification and analysis of ATF property management system data

We determined for each item verified whether the user and location fields were accurate in the property management system. Of the

<sup>48</sup> A property confirmation memorandum was a document we used to verify property that was not physically available for verification because the personnel in possession of the property were out of the office during our visit. We left confirmation memoranda for these personnel to list property in their possession, have a supervisor confirm the property, and send to us.

1,316 items we found that 217 (16 percent) had an incorrect user, incorrect location, or both in the property management system record, or the item was not included in the property management system at all. The total number of verified items with incorrect records are detailed in the following chart.

**NUMBER OF PROPERTY MANAGEMENT SYSTEM ERRORS AND ERROR RATE FOR VERIFIED ITEMS**



Source: OIG verification and analysis of ATF property management system data

We identified 1 weapon and 11 laptop computers in the Atlanta Field Division and 4 laptop computers in the Washington Field Division that ATF staff had not entered into the property management system.

ATF implemented a new automated property management system during 2004, but its property management policy was not updated to reflect implementation of the new system until April 2008. Consequently, the processes outlined in the policy were outdated between 2004 and April 2008.

*Additional Audit Testing (Phase II)*

Because our preliminary audit work determined that data within the property management system was inaccurate and incomplete, we performed additional testing at other ATF offices. During this phase, we statistically selected weapons and laptop computers from the property management system and physically verified each item at selected field and headquarters offices.

We selected a statistical sample of 935 weapons and 560 laptop computers from the property management system and physically attempted to verify each item. The statistical sample and locations were selected by an analysis based on quantity of personnel, weapons, and laptop computers. We verified property and evaluated property records and property management activities at the following locations: ATF headquarters divisions in Martinsburg, West Virginia; Landover, Maryland; and Glynco, Georgia; and divisional offices in Kansas City and St. Louis, Missouri; Las Vegas, Nevada; Little Rock, Arkansas; Los Angeles, Riverside, and San Francisco, California; Metairie and Shreveport, Louisiana; and Philadelphia and Pittsburgh, Pennsylvania.<sup>49</sup>

ATF was unable to provide all weapons and laptop computers for our verification. The weaknesses appear to be localized in certain offices, as reflected in the following table, which summarizes the results of verification testing at each selected location. We added the Phase I results for comparison purposes.

---

<sup>49</sup> 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.

**SAMPLE TESTING**

Location	WEAPONS		LAPTOP COMPUTERS	
	Accounted For	Unaccounted For	Accounted For	Unaccounted For
<b>PHASE I</b>				
Atlanta Field Division (FD)	331	0	237	1
Washington FD	519	3	229	5
<b>PHASE I TOTALS</b>	<b>850</b>	<b>3</b>	<b>466</b>	<b>6</b>
<b>PHASE II</b>				
Headquarters				
Glynco, GA (HQ)	92	0	67	2
Landover, MD (HQ)	0	0	31	0
Martinsburg, WV (HQ)	165	0	58	0
Kansas City FD				
Kansas City, MO	58	0	53	0
St. Louis, MO	84	0	30	2
Los Angeles FD				
Los Angeles, CA	96	1	49	12 <sup>50</sup>
Riverside, CA	31	0	16	0
New Orleans FD				
Little Rock, AR	36	0	21	0
Metairie, LA	59	0	36	1
Shreveport, LA	46	0	18	0
Philadelphia FD				
Philadelphia, PA	77	0	48	0
Pittsburgh, PA	66	0	35	0
San Francisco FD				
San Francisco, CA	64	0	56	0
Las Vegas, NV	60	0	25	0
<b>PHASE II TOTALS</b>	<b>934</b>	<b>1</b>	<b>543</b>	<b>17</b>

Source: OIG verification and analysis of ATF property management system data

As with the first phase of our testing in the Atlanta and Washington Filed Divisions, for the statistically selected sample in other ATF offices we physically verified the item or verified it by confirmation memoranda.

We also tested the completeness of the property records by selecting a judgmental sample of staff at seven offices and tracing property in their possession to the property management system to determine if property management system records were correct.<sup>51</sup> The results of our review are summarized in the following table.

<sup>50</sup> ATF staff in the Los Angeles office believed 12 unaccounted for laptop computers had been donated, but they could not provide copies of the donation forms.

<sup>51</sup> We performed this test at seven locations because all personnel at the other locations were already included in the sample.

**PERSONNEL PROPERTY TO PROPERTY MANAGEMENT SYSTEM TESTING**

Location	Personnel Selected	WEAPONS		LAPTOP COMPUTERS	
		Number Belonging to Personnel Selected	Records Incorrect in Property Management System	Number Belonging to Personnel Selected	Records Incorrect in Property Management System
Glynco (HQ)	2	3	0	1	0
Martinsburg (HQ)	5	0	Not Applicable	5	1
Kansas City	6	3	1	6	1
Los Angeles	6	12	1	6	1
Metairie	5	13	0	5	1
Philadelphia	5	6	0	5	0
St. Louis	4	7	0	5	0
<b>TOTALS</b>	<b>33</b>	<b>44</b>	<b>2<sup>52</sup></b>	<b>33</b>	<b>4<sup>53</sup></b>

Source: OIG verification and analysis of ATF property management system data

During these tests, we identified items for which conflicting information was entered in the property records.<sup>54</sup> For instance, a record's data elements for "office code" and "location" contained conflicting information, indicating an item was located in two different places. An ATF official explained how this may occur. He said that when an item is transferred the "office code" field is automatically updated in the record when the receiving location accepts the property in the property management system, but the "location" field must be manually updated. In these cases, the receiving location does not manually update the location field.<sup>55</sup> We believe that the automated system should be used to prevent

<sup>52</sup> One weapon in Kansas City was assigned to another individual and one weapon in Los Angeles listed an incorrect location.

<sup>53</sup> One laptop computer was assigned to another user and location in Martinsburg. One laptop computer in Kansas City was not in the property management system. One laptop computer in Los Angeles listed an incorrect location. One laptop computer in New Orleans did not have a user listed.

<sup>54</sup> The property management system database contains data elements to record the office the item is assigned to and the location where it can be found, as some offices operate in multiple locations. Those elements are related because property that is assigned to a specific office should be found in a limited set of locations.

<sup>55</sup> When a property item is transferred, the sending office's property custodian sends an e-mail through the property management system identifying the property to be transferred to the receiving office's property custodian. When the receiving property custodian electronically accepts the new property, the office code database field is automatically updated in the property management system to reflect the receiving location office code.

conflicting information by applying relationship edits between related data elements. For laptop computer records, ATF may be able to interface with the leasing contractor's tracking system to maintain more accurate records.

## **Encryption**

As discussed in Finding I, in March 2007 the Chief Information Officer in ATF's Office of Science and Technology issued a memorandum to all ATF employees explaining the importance of safeguarding laptop computers. The memorandum stated that ATF would be implementing new security measures to encrypt laptop computer hard drives. This effort was intended to provide an additional layer of protection to help maintain confidentiality of the data stored on laptop computers. ATF staff began installing the encryption software for laptop computers in May 2007, and as of April 2008 ATF staff told us they had completed the installation on all networked laptop computers. On April 22, 2008, ATF staff reported that they had installed encryption software on all 5,774 networked ATF laptop computers. The majority of ATF laptop computers are networked and assigned to individuals as personal property. ATF has approximately 1,800 stand-alone laptop computers. ATF staff planned to encrypt these standalone laptop computers and provided disks to staff to install the encryption software.

During our review of property in Phases I and II, and prior to ATF's reported completion of the encryption software installation, we tested to determine if ATF had installed encryption software on sampled laptop computers. Sixty-three of the 1,065 laptop computers we tested did not have the encryption software installed at the time of our tests. However, 42 of the 63 unencrypted laptop computers were used strictly for a dedicated purpose such as Global Positioning System tracking or video surveillance and ATF staff told us they do not store sensitive information on those laptop computers. The remaining 21 unencrypted laptop computers were assigned to users. Of those 21 unencrypted laptop computers:

- 17 were located in the Washington Field Division;<sup>56</sup>
- 3 were located in the Atlanta Field Division; and
- 1 was located in the Los Angeles Field Division.

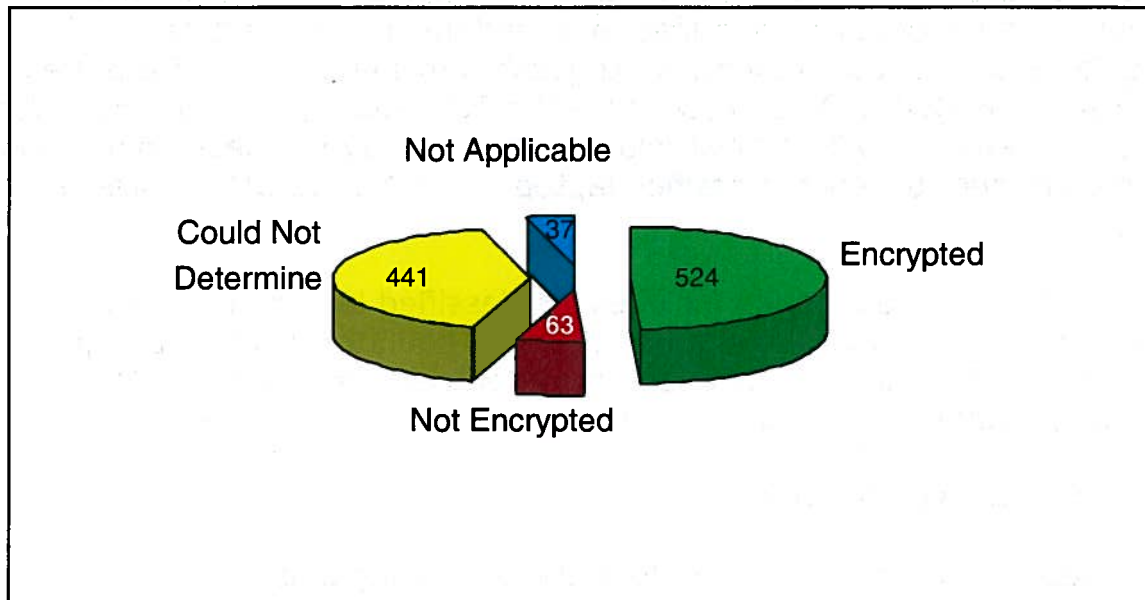
---

<sup>56</sup> We conducted testing in the Washington Field Division shortly after ATF began installing the encryption software.



We could not determine the encryption status for the 180 laptop computers we verified by confirmation memoranda or the 238 we physically verified but a user was not available to log on and show us that the encryption software was installed. The remaining 23 laptop computers could not be tested because they were unaccounted for. The encryption status results are summarized in the following chart.

**ENCRYPTION SOFTWARE TESTING AS OF DECEMBER 2007**



Source: OIG testing of ATF laptop computers

Section 3.13 of DOJ's Information Technology Security Standard 1.6, Classified Laptop and Standalone Computers Security Policy, issued November 1, 2006, requires that all classified information on laptop and standalone computers be encrypted. We determined 5 of ATF's 18 classified laptop computers we tested were not encrypted. By not encrypting these classified laptop computers, ATF did not comply with DOJ policy and risked compromising classified information if the laptop computer were lost, stolen, or missing. Two of the unencrypted laptop computers had classified information on the hard drives at the time of our test. One of the unencrypted laptop computers was not labeled with a Property Identification Number and could not be found in the property management system. Therefore, if the laptop computer was lost, stolen, or missing there would be no record that ATF ever had it and classified information could be compromised.

As of April 2008, ATF was in the process of installing encryption software on the five classified laptop computers. However, ATF did not

provide a reason why these five classified laptop computers had not been encrypted up to this point.

### **Reporting Requirements for Laptop Computers Containing Classified Information**

Beginning March 31, 2004, the DOJ's Office of the Chief Information Officer required ATF to report the number of laptop computers it has authorized for processing classified information. To ensure that ATF complied with the requirement, we requested this information from the DOJ CIO. The DOJ CIO had received ATF's 2007 submission, but none for any prior years. An ATF official told us that ATF may not have known about the requirement to report classified laptop computers to DOJ in previous years.

ATF's 2007 submission included 13 classified laptop computers. However, during our audit we found that ATF had 18 classified laptop computers. The additional five laptop computers were the same five described above as being unencrypted.

### **Reporting Losses to DOJ**

Section 11.c of DOJ Order 2630.2A, Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures, and Justice Property Management Regulations 128-1.5305, requires all components, including ATF, to submit to DOJ's Justice Management Division (JMD), semiannual reports summarizing thefts and losses of government property during the preceding 6 months. ATF has never submitted a semiannual report summarizing thefts of government property. However, during the period October 9, 2002, through July 24, 2007, ATF experienced the loss or theft of 76 weapons and 418 laptop computers. JMD sent follow-up correspondence to ATF in 2005, 2006, and 2007 reminding it to submit the semiannual reports. We have asked JMD about this and are awaiting their response. ATF submitted its first semiannual report to JMD in April 2008.

The ATF's Chief for Materiel Management told us that ATF had not submitted previous semiannual reports because the property management system did not allow ATF to consolidate the loss information. He further explained that ATF was in the process of updating the property management system to be able to consolidate the loss information.

Although ATF's property management system may not have been able to consolidate loss information, it appears to us that ATF did have the resources to compile lists of lost, stolen, or missing items. For example, ATF could have used the disposed records database, Report of Surveys, and Internal Affairs reports to compile lists of lost, stolen, or missing property to meet the JMD reporting requirement.

#### *Department of Justice Computer Emergency Response Team*

We tested whether ATF reported lost, stolen, or missing laptop computers to DOJCERT. We identified 53 laptop computer losses that were reported to Internal Affairs, of which 16 occurred prior to the DOJCERT reporting requirement, leaving 37 incidents that should have been reported. We found that 21 of the 37 were reported to DOJCERT, while 16 were not reported as required.

We asked ATF officials why the 16 incidents of lost, stolen, or missing laptop computers were not reported to DOJCERT, but as of July 2008 we had not received a response. Of the 16 laptop computers not reported to DOJCERT, ATF reported that 3 contained sensitive information, 6 did not contain sensitive information, and ATF could not determine whether 7 contained sensitive information. Eleven of the 16 laptop computers were not encrypted because ATF began installing encryption software after these laptop computers were lost, stolen, or missing. Two may have been encrypted because they were lost, stolen, or missing after ATF began installing encryption software. ATF reported that one of those laptop computers had sensitive information and the other did not. We could not determine the encryption status for the remaining three laptop computers because we could not determine the dates the losses occurred.

#### **Disposal of Weapons and Laptop Computers**

ATF's process for disposing of weapons and laptop computers consists of the following steps.

- The property custodian notifies the property management representative of any excess property.

- The property management representative completes an ATF Form 1854.1, Declaration of Excess Property, and forwards it to the Property Accountable Officer.<sup>57</sup>
- The property accountable officer reports the excess property to the General Services Administration (GSA).
- GSA screens the property for transfer to other federal agencies, donation to state agencies or other authorized recipients, or offers the property for sale to the public.<sup>58</sup>
- The property accountable officer sends disposal instructions and a Transfer Order (SF 122) to the property custodian.
- Before computers are donated, the property custodian and property accountable officer ensure the hard drives are cleared and a Certificate of Data Clearing (ATF Form 1854.2) is prepared.
- The property custodian obtains signatures from the receiving organization on Transfer Order (SF 122), if donated, and forwards the Transfer Order and Certificate of Data Clearing to the property accountable officer.
- The property accountable officer adjusts the property records.

We selected a representative sample of 121 of 3,982 weapons and 176 of 4,701 laptop computers disposed of during the audit's 59-month time frame. While not statistically selected, the sample is a representative sample because it includes disposals from headquarters and field divisions, disposals occurring during each year of the audit period, and all methods of disposal. Disposed weapons and laptop computers are destroyed, transferred to another agency, lost, missing, or stolen, exchanged, donated, returned, or removed from the active property records as an inventory adjustment. The number of items for each type of disposal are summarized in the following table.

---

<sup>57</sup> At headquarters the property management representative completes an ATF Form 1630.1, Facilities Service Support Form, and ATF Form 1851.1, Property Transfer Record, and forwards the forms to the property accountable officer who removes the property from the property management system.

<sup>58</sup> Weapons can only be sold to the public after they have been rendered permanently inoperative.

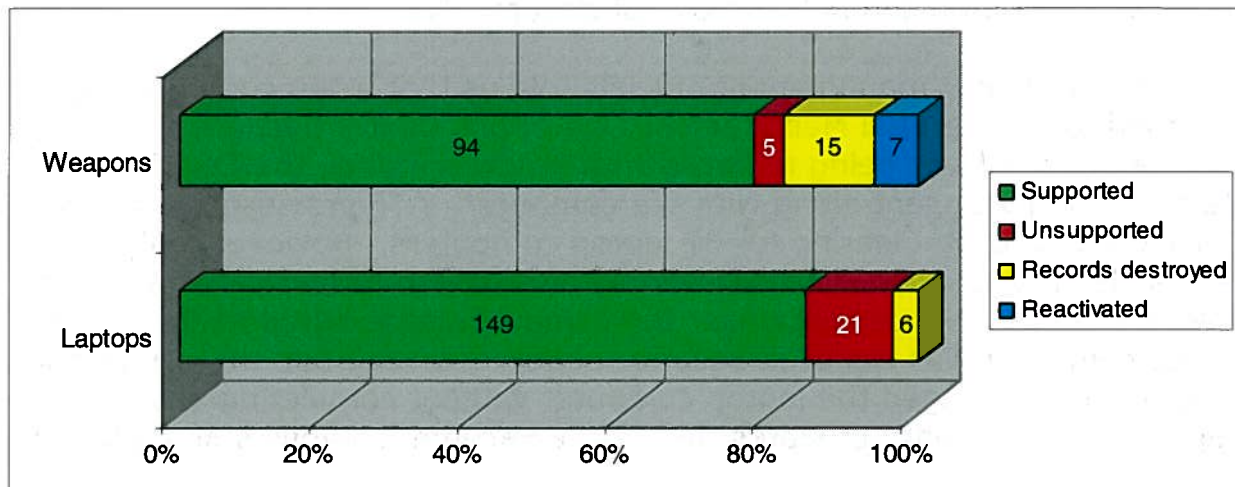
### DISPOSED PROPERTY TESTING

DISPOSAL TYPE	WEAPONS	LAPTOP COMPUTERS
Destroyed	63	19
Transferred	39	34
Lost, Missing, or Stolen	6	24
Exchanged	4	7
Donated	1	70
Inventory Adjustment	7	17
Returned	1	4
Could Not Determine <sup>59</sup>	-	1
<b>TOTALS</b>	<b>121</b>	<b>176</b>

Source: ATF Disposed Property Records

To test the controls of the disposal process, we examined whether the sample of 297 items included the proper support documentation such as a Report of Destruction (ATF Form 1850.2), Transfer Document, or Report of Survey and contained the appropriate signatures for each disposal. The following chart details whether ATF provided proper documentation for the disposed weapons and laptop computers in our sample.

### SAMPLE DISPOSED PROPERTY TESTING<sup>60</sup>



Source: ATF disposed property records

Ninety-five percent (94 of 99) of the weapons and 88 percent (149 of 170) of the laptop computers removed from the active property records were adequately supported by documentation containing the required

<sup>59</sup> We could not determine the reason for disposal from ATF records.

<sup>60</sup> ATF has a 3-year document retention policy for property records. As a result, we were unable to verify disposal documents for all items selected that ATF disposed of prior to FY 2005.

signatures.<sup>61</sup> Officials at the Property Management Office told us that the records supporting the disposal of 5 weapons and 10 laptop computers were misplaced when ATF moved to its new headquarters building in August 2007.

Two laptop computers did not include all required signatures and nine laptop computers did not have the Property Identification Numbers listed on the disposal documents. In our judgment, the effect of these errors is not significant.

Before laptop computers are disposed of, the property custodian and the property accountable officer should ensure the hard drives are cleared and a Certificate of Data Clearing is prepared, as required by ATF policy. Of the 149 supported laptop computer disposals, we tested 116 to determine whether the data clearing was supported by appropriate documentation. We did not test the remaining 33 because the laptop computers were inventory adjustments, lost, stolen, or transferred to the Treasury Tax and Trade Bureau and no there were no actual laptop computers to clear.<sup>62</sup> ATF provided a Certificate of Data Clearing for only 4 (3 percent) of the 116 laptop computers we tested. The data clearing status for 97 percent of the disposed laptop computers was not documented.

ATF property management officials told us that when computers were returned to the Materiel Management Operations Center because the item was defective or was being replaced with a newer model, the Certificate of Data Clearing was sent along with the computer. ATF provided electronic Certificates of Data Clearing for 32 laptop computers. However, only one certificate was for an item in our sample of disposed property. An Internal Affairs manager told us that under the computer lease agreements, when a laptop computer was replaced because of defect or upgrade the contractor's technicians exchanged the laptop computer without completing any paperwork. The contract states that if a replacement involves non-volatile

---

<sup>61</sup> We excluded seven weapons from testing because property records for those weapons were reactivated when the weapon was found or when it was discovered that the wrong record had been deleted. We also excluded 15 weapons and 6 laptop computers from testing because the supporting documentation had been destroyed in accordance with ATF's record retention practices.

<sup>62</sup> Only the law enforcement offices of the ATF transferred to the Department of Justice in January 2003.

memory, the contractor should erase all sensitive data before parts removal, provided the laptop computer is operational.<sup>63</sup>

In addition, as discussed previously, for several years annual ATF inventories resulted in large numbers of laptop computers that could not be accounted for and in 2006 ATF began removing those missing items from its active property records. The Internal Affairs manager did not know whether the hard drives of these computers were cleared of any sensitive information that may have been on the laptop computers removed from the property records as inventory adjustments.

We compared the active property records to the disposed property records and found that 28 weapons and 197 laptop computers were contained in both active and disposed property records. An ATF official explained that if ATF does not locate an item during an inventory, Materiel Management staff removes the item from the active records and records it in the disposed records. If the item is located during a subsequent inventory, Materiel Management staff place the item back into the active records, but do not remove the item from the disposed records. The explanation is reasonable as to why an item may be in both active and disposed records. However, an item should not be recorded as both active and disposed and ATF should adjust the entry in the disposed records to note that the item was reactivated. We also found that 124 items had multiple disposal dates that included items with multiple types of disposal.

ATF did not have proper controls over disposed property nor did it provide support documentation for 5 disposed weapons and 21 disposed laptop computers. In addition, ATF did not provide documentation supporting the data clearing for 112 disposed laptop computers. Since ATF included items in both disposed and active property records, ATF did not follow established procedure to update disposed records to reflect reactivation. As a result, ATF could not determine whether the item was active or disposed. We recommend that ATF maintain support documentation for all disposed property, document data clearing of disposed laptop computers, and update active and disposed property records.

---

<sup>63</sup> Non-volatile memory is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, and most types of magnetic computer storage devices such as hard disks, floppy disks drives, and magnetic tape.

## **Exit Procedures for Departing Employees**

The clearance process for departing employees begins when they notify their supervisor of their intent to leave ATF or when the supervisor notifies employees of a termination. The supervisor initiates an ATF Form 2391.1, Separation Checklist. The supervisor or other designated official should coordinate with the property custodian to ensure that employees return property for which ATF issued an ATF Form 1854.4 or 1854.4A, Property Issue Receipt. On or before employees' last day of employment, the supervisor or other designated official should collect property issued including weapons, ammunition, and laptop computers. Weapons and agency-issued ammunition are to be returned to the division director, SAC, or tactical operations officer in accordance with ATF Order 3000.8, ATF's weapons policy. The supervisor should complete and sign the Separation Checklist and provide copies to the employee and to the personnel office.

To test whether all assigned property had been returned by separated ATF employees, we judgmentally selected 30 former ATF employees from 12 locations where we performed other tests. We asked ATF staff for the 30 separation checklists, of which ATF staff could provide only 6. Each checklist contained only a statement certifying that the supervisor received all property from the employee and did not identify specific property items returned by the employee. We were also not able to use the property management system to identify items that had been associated with each separated employee. Although the system contains historical information about employees to whom property was previously assigned, those property records can only be retrieved using property identification numbers. Consequently, we were unable to perform the test to ensure separating employees had returned all weapons and laptop computers assigned to them during ATF service.

We were able to test whether the property management system still contained property records showing items assigned to separated employees. Our analysis identified 26 active weapons and 152 active laptop computers assigned to persons who had separated from ATF. This occurred because ATF staff did not update the property management system to reflect whether the items were returned.

## **Conclusion**

Our audit identified weaknesses in ATF's control over weapons and laptop computers in several areas. We found that ATF failed to adequately: (1) maintain accurate and complete records in the property management



system and update the system to reflect administrative changes occurring during inventories; (2) locate all active weapons and laptop computers sampled for review; (3) report to the DOJ's Office of the Chief Information Officer the number of laptop computers authorized to process National Security Information; (4) report all weapon and laptop losses to DOJ and all laptop loss incidents to DOJCERT; (5) maintain support documentation for disposed weapons and laptop computers and ensure that ATF clear computer hard drives prior to disposal; and (6) maintain documentation showing ATF collected all weapons and laptop computers from separating employees. Consequently, we make several recommendations for ATF to improve its management of weapons and laptop computers.

### **Recommendations**

We recommend that ATF:

6. Develop procedures for updating the property management system to ensure accurate and complete weapons and laptop computer records are maintained.
7. Locate or report as missing all sampled items not found during the audit.
8. Ensure all laptop computers are encrypted.
9. Ensure complete, accurate, and timely reports are submitted to the DOJ CIO containing all appropriate ATF laptop computers authorized to process classified information.
10. Ensure complete, accurate, and timely semiannual reports identifying lost, stolen, or missing weapons and laptop computers are submitted to the DOJ Security Officer and JMD.
11. Develop procedures to ensure ATF completes accurate, and timely incident reports summarizing the loss of ATF laptop computers and submits those reports to DOJCERT, as required by DOJ policy.
12. Maintain documentation for all disposed property, document data clearing of disposed laptop computers, and update active and disposed property records, as necessary.

13. Develop procedures and maintain documentation to ensure that separated employees return all weapons, laptop computers, and other accountable property before they separate from ATF.

### **III. INTERNAL CONTROLS OVER AMMUNITION AND EXPLOSIVES**

We concluded that ATF had adequate physical security over both ammunition and explosives. Its inventory controls over explosives were far better than those for ammunition. ATF maintained perpetual inventory records at explosives magazines and we were able to verify the quantities of explosives on hand. In addition, ATF staff conducted independent inventories of explosives magazines during internal inspections.

Recordkeeping for ammunition was less consistent. Nine of the 20 offices we tested did not maintain perpetual inventories of ammunition as required by ATF policy. Of the 11 offices that maintained perpetual records, 4 had significant inaccuracies in the records, 1 of which had 478,400 fewer rounds of ammunition in stock than was recorded on the perpetual inventory. ATF also was not enforcing its policy that field offices conduct annual ammunition inventories and submit the results to ATF's Materiel Management Branch. It appeared that no office had ever submitted an annual ammunition inventory to ATF headquarters, nor had ATF taken any follow-up action to obtain annual ammunition inventories. ATF officials could not explain the absence of perpetual inventories or for not ensuring that annual ammunition inventories are conducted and submitted to headquarters. Without inventory controls over ammunition, ATF is subject to the loss or theft of ammunition without detection.

#### **Ammunition Controls**

In 2002, the Treasury OIG reported that ATF had limited written policies regarding controls over ammunition, no standard recordkeeping, and no physical inventories. As a result of the Treasury audit, ATF implemented new policies that required all divisions and the ATF Academy to conduct a baseline inventory of all ammunition, and report the results to the Property and Fleet Management Section of the Materiel Management Branch. The memorandum also established a requirement for an annual inventory of all ATF-owned ammunition and required a perpetual inventory system for ammunition. It also required an annual inventory of all ATF-owned ammunition and that a disinterested person assist in conducting all inventories.

We sought to review the last two annual inventories of ammunition submitted to the Chief of the Property and Fleet Management Section, but we were unable to perform the review because ATF could not produce

documentation for any of the inventories. We asked ATF officials why the inventory records were not available, but as of July 2008 ATF had not responded.

We also reviewed ammunition controls at 20 ATF offices where we tested weapons and laptop computers. Of the 20 offices, we found that 11 kept perpetual inventory records as required and 9 did not. At each location, we compared the perpetual records for each type of ammunition to the actual inventory stored at the office. We noted that five of the offices had accurate perpetual record systems and six offices had inaccurate records. One office had inaccuracies in all but one type of ammunition that was short 478,400 rounds. We attributed the large shortage to inadequate recordkeeping. The perpetual record was apparently not updated as transactions occurred. The official responsible for the ammunition believed the missing ammunition had probably been given to the military. While this may be correct, ATF has no way of knowing what happened to the missing ammunition without a record of the transactions. Nine offices did not keep perpetual records at all. Our results are summarized in the following table.

**AMMUNITION RECORDS TESTING**

Location	Summary of Ammunition Records		
	Perpetual Records Kept?	Records Accurate?	Description of Inaccuracies
Atlanta, Georgia	No	N/A	Atlanta did not keep any ammunition records.
Macon, Georgia	No	N/A	Macon did not keep any ammunition records.
Savannah, Georgia	No	N/A	Savannah did not keep any ammunition records.
Richmond, Virginia	Yes	Yes	N/A
Bristol, Virginia	Yes	Yes	N/A
Roanoke, Virginia	Yes	Yes	N/A
Norfolk, Virginia	Yes	No	Shortage of seven cases of .40 caliber ammunition.
Martinsburg, West Virginia	Yes	No	Shortage of one case of .40 caliber ammunition.
Glynco, Georgia	Yes	Yes	N/A
Headquarters	Yes	No	Perpetual records did match actual inventory for 19 of 20 types. One caliber had a shortage of 478,400 rounds.
Kansas City, Missouri	Yes	No	Shortage of 10 cases of .40 caliber ammunition.
Las Vegas, Nevada	No	N/A	Las Vegas began documenting inventory records just prior to the audit site visit.
Little Rock, Arkansas	Yes	Yes	N/A
Los Angeles, California	No	N/A	Los Angeles began documenting inventory records on 10/15/2007, just prior to the audit site visit.
San Francisco, California	No	N/A	San Francisco began documenting inventory records just prior to the audit site visit.
New Orleans, Louisiana	No	N/A	New Orleans began documenting inventory records just prior to the audit site visit.
Shreveport, Louisiana	Yes	No	Shortage of seven cases of .223 caliber ammunition. According to the office, this ammunition was issued during the aftermath of Hurricane Katrina. No specific records were kept of this distribution.
Philadelphia, Pennsylvania	No	N/A	Philadelphia only logged ammunition used. No baseline was established.
Pittsburgh, Pennsylvania	No	N/A	Pittsburgh did not keep any ammunition records.
St. Louis, Missouri	Yes	No	Shortage of one case of .40 caliber ammunition.

Source: OIG analysis of testing at ammunition inventories

The nine offices that did not keep perpetual inventories and the one office that had significant deficiencies in its perpetual inventory system did not follow procedures to accurately account for all stored ammunition. One office did not keep complete perpetual records because an agent who worked in the office believed that the requirement to keep the perpetual records and submit annual inventories had been rescinded. We asked ATF's Chief Financial Officer to provide information confirming that the requirement had been rescinded. As of July 2008, we had not a received response.

### *Reconciling Ammunition Records to the Financial System*

During our review, we judgmentally selected 12 ammunition shipments to 8 locations where we performed testing. The disbursements were for .223 caliber ammunition shipped between September 26, 2006, and April 11, 2007. We attempted to trace these shipments of ammunition to the perpetual inventory records that were to be maintained at these locations. However, none of the 12 shipments made to the 8 locations where we performed testing were recorded in the perpetual inventory records. Although ATF policy requires the maintenance of perpetual records, five of the eight locations did not keep ammunition inventory records. At two of the other field offices, records were retained for only the last year, a period that did not include the shipments. In the eighth location, which was the headquarters ammunition facility, an agent told us that the shipment may have been intended for the Baltimore office. Since the receiving location for the Baltimore office is the headquarters facility, that shipment would have been picked up by the Baltimore office and logged into that office's inventory.<sup>64</sup> Unless ATF offices maintain complete and accurate perpetual records, ATF cannot ensure it has received all the ammunition that it has paid for or that ammunition has not been lost, stolen, or missing.

### *Physical Security*

Ammunition was stored in various locations at the different ATF offices that we tested. Smaller ATF field offices kept ammunition in vaults within the office space and access to the vaults was controlled by key cards and alarm systems. Agents had access to these vaults. Larger field offices and divisions kept ammunition in warehouse facilities or at a firing range. The

---

<sup>64</sup> We did not verify whether the ammunition was logged into the Baltimore office's inventory. However, when the headquarters facility received the ammunition it should have recorded the ammunition in its inventory and then removed the ammunition from its inventory once the Baltimore office retrieved the ammunition.

warehouse facilities stored other equipment in addition to ammunition. Not all agents had access to these facilities. The following photograph shows ammunition stored in a vault located in the basement of ATF office space. The vault was padlocked and had a security system.

#### **AMMUNITION STORAGE**



Source: OIG photograph of ATF storage of ammunition

The next photograph shows ammunition in an ammunition storage facility for a larger division. The storage facility was an ATF-owned warehouse that also housed ATF vehicles and tactical equipment.

## **AMMUNITION STORAGE**



Source: OIG photograph of ATF storage of ammunition

Treasury's 2002 audit reported that ATF had satisfactory procedures for ensuring the physical security of its ammunition, and we found that ATF continued to have proper physical security of its ammunition.

### **Explosives Controls**

The Treasury OIG reported in its 2002 audit that controls over physical inventories of explosives lacked independent review. In response to the finding, ATF required that a disinterested person participate in all future inventories of explosives magazines. In addition, ATF mandated that a perpetual record of each type of ATF-owned explosive be maintained.

ATF Memorandum 3325, dated May 14, 2002, required an annual inventory of all explosives located in ATF magazines. Also, the memorandum explained that ATF divisions must keep a Daily Summary of Transaction Record to be used as a perpetual inventory for each explosives magazine. In addition, the ATF Explosives Industry Operations Section conducted annual inspections of all ATF magazines, which included an inventory review by persons independent of daily responsibility for the magazine. In addition, ATF's Explosives Industry Operations Section performs annual inspections of all ATF explosives magazines that include



physical inventories by “disinterested persons” who are independent of daily responsibility for the magazine.

We reviewed explosives at 16 ATF locations and found that each kept perpetual inventory records as required. At each location, we compared the perpetual records for each type of explosive to the actual inventory stored at the location. We found that the explosives on hand did not correspond with the amounts recorded in the perpetual records at 8 of 16 locations. Our results are summarized in the following table.

**EXPLOSIVES RECORDS TESTING**

Location	Summary of Explosives Records		
	Perpetual Records Kept?	Records Accurate?	Description of Inaccuracies
Atlanta, Georgia	Yes	No	Overage of 9 pieces of 1-pound booster.
Leesburg, Virginia	Yes	Yes	N/A
Falls Church, Virginia	Yes	Yes	N/A
Bristol, Virginia	Yes	Yes	N/A
Chantilly, Virginia (Explosives Technology Branch)	Yes	Yes	N/A
Fort A.P. Hill, Virginia (Three magazines)	Yes	No	Shortage of two weatherproof fuse lighters.
Front Royal, Virginia (Six magazines)	Yes	No	Overage of 18 cases of ammonium nitrate and an overage of 1,250 feet cord explosive.
Millersville, Maryland (Explosives Technology Branch)	Yes	Yes	N/A
Kansas City, Missouri	Yes	No	Overage of three cast boosters.
Little Rock, Arkansas	Yes	Yes	N/A
Los Angeles, California	Yes	No	Overage of one item. Another item was incorrectly classified on the inventory records.
San Francisco, California	Yes	No	Shortage of one 6-gram slip on booster.
New Orleans, Louisiana	Yes	No	Shortage of two cast boosters.
Reading, Pennsylvania (Philadelphia Field Division)	Yes	No	Overage of one piece of slurry explosive.
Camden, New Jersey (Philadelphia Field Division)	Yes	Yes	N/A
St. Louis, Missouri	Yes	Yes	N/A

Source: ATF explosives inventory records

We concluded that ATF's control over explosives was adequate because all offices kept perpetual explosives inventory records as required. However, as shown in the preceding table, three magazines were missing several pieces of explosives and five magazines had more pieces of explosives than were recorded on their perpetual inventory records. We considered the missing items as minor discrepancies. One magazine had an overage in stock of 9 pieces of an item and another had overages of 18 pieces of one item and 1,250 feet of another item.

#### *Reconciling Explosives Records to the Financial System*

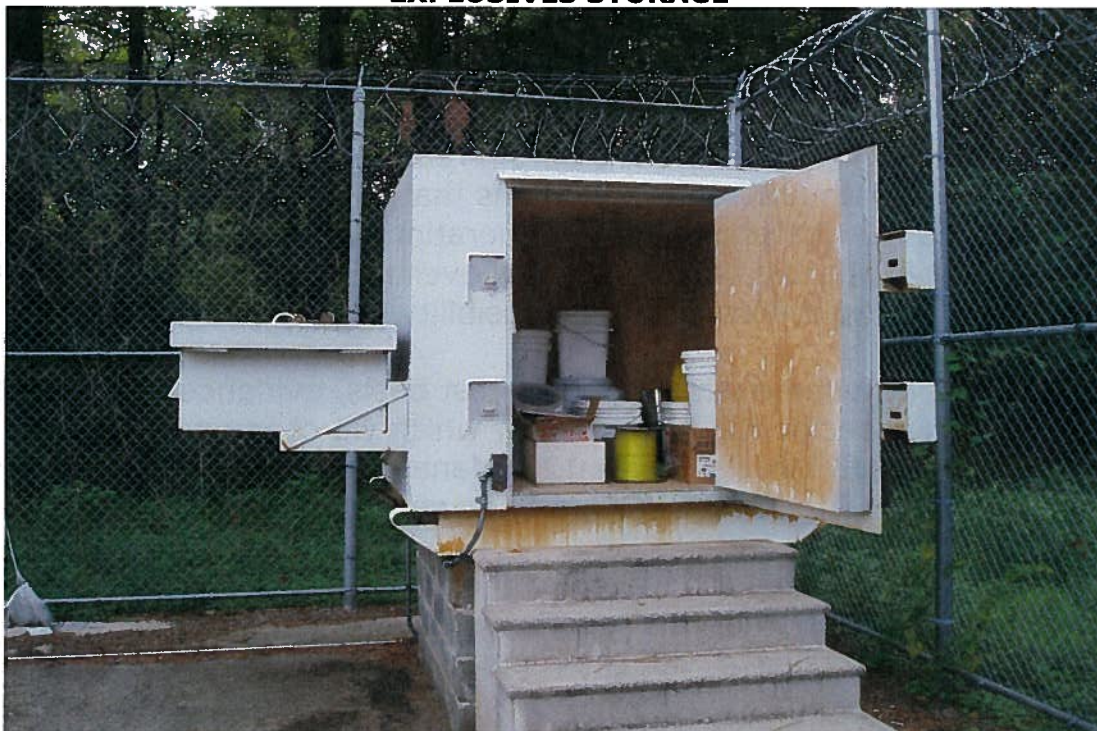
We reviewed the only two purchases for explosives that occurred within our audit period, both of which were sent to the K-9 Training facility at Front Royal, Virginia. We were able to trace both shipments from the invoices to the perpetual log kept with the magazines at Front Royal.

#### *Physical Security*

ATF's Explosives Industry Operations Orange Book, Federal Explosives Law and Regulations, regulates how explosives are to be stored. An ATF official told us that only certified personnel had access to explosives magazines. In addition, ATF Memorandum 5400 requires an independent physical security review completed by the ATF's Industry Operations. Industry Operations reviewed whether each magazine adhered to structural specification and access requirements. We reviewed inspection reports and confirmed that magazines met the structural requirement and the magazines we reviewed were all secured. Therefore, we found that ATF's physical controls over explosives were adequate.

The following photo shows an explosives magazine which was located in a fenced area surrounded by barbed wire. The magazine's door also had a double lock.

## EXPLOSIVES STORAGE



Source: OIG photograph of ATF explosives magazine

### Conclusion

We concluded that ATF's controls over explosives were adequate. However, we identified continued weaknesses in controls over ammunition. Although ATF developed written procedures to enhance controls over ammunition in response to the 2002 Treasury audit, ATF failed to enforce its policy. Specifically, ATF did not perform annual inventories of ammunition and did not maintain accurate and complete perpetual inventory records of ammunition.

### Recommendation

We recommend that ATF:

14. Enforce current requirements to perform annual inventories of ammunition and maintain a perpetual inventory system at all ammunition storage locations to ensure accurate and complete records.

## **STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS**

The audit of ATF's controls over weapons, laptop computers, ammunition, and explosives was conducted in accordance with the *Government Auditing Standards*. As required by these standards, we tested selected transactions and records to obtain reasonable assurance about ATF'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 ATF's control over weapons laptop computers, ammunition, and explosives 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.

Except for instances of non-compliance identified in the Findings and Recommendations section of this report, we did not identify any other instances of non-compliance with the regulations cited above.

## APPENDIX I

### OBJECTIVES, SCOPE, AND METHODOLOGY

We completed an audit of ATF's control over weapons, laptop computers, ammunition, and explosives. The purpose of the audit was to determine: (1) the adequacy of the ATF's actions taken in response to weapons, laptop computers, ammunition, and explosives identified as lost, stolen, or missing; and (2) the effectiveness of the ATF's internal controls over weapons, laptop computers, ammunition, and explosives.

We performed the audit in accordance with the *Government Auditing Standards* and included such tests of the records and procedures that we considered necessary. Our testing generally covered the period between October 1, 2002, and August 31, 2007.

We observed the control environment for weapons and laptop computers from the Materiel Management Division at ATF headquarters. We also observed the control environment for ammunition and explosives from the Training and Professional Development and the Explosives Industry Operations Divisions at ATF headquarters. We performed on-site audit work between July 2007 and April 2008 at ATF headquarters (including the training facilities in Front Royal and Fort A.P. Hill, Virginia, and Glynco, Georgia and division branches in Martinsburg, West Virginia) and at field offices in Atlanta, Georgia; Kansas City, Missouri; Las Vegas, Nevada; Little Rock, Arkansas; Los Angeles, Riverside, and San Francisco, California; New Orleans and Shreveport, Louisiana; Philadelphia and Pittsburgh, Pennsylvania; St. Louis, Missouri; and Washington, D.C.

To examine ATF's efforts to identify lost, stolen, or missing weapons, laptop computers, ammunition, and explosives, we obtained documentation of such losses that had occurred since October 1, 2002, and reviewed the available files and the circumstances surrounding those losses. For lost, stolen, or missing weapons, we queried NCIC to determine if those losses had been reported and if weapons had been subsequently recovered.

For laptop computers, we sought to determine if the loss resulted in compromised classified or sensitive information. We could not independently verify the sensitivity of the information lost. Therefore, we relied on statements from investigative reports and from information reported to DOJCERT for each lost, stolen, or missing laptop to ascertain whether classified or sensitive information was compromised.

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 October 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;
- receipt and assignment, including weapons and laptop computers not assigned to specific individuals (pooled property), 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 22,476 weapons and 7,505 laptop computers reported in the property management system as of August 2007. In total, we reviewed 2,823 items, including 1,790 weapons and 1,033 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 purchased between October 1, 2002, and August 31, 2007, as recorded in purchase documents, to ensure that the items were recorded in the property management system;
- 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 ATF location to ensure that the item was accurately reflected in the property management system; and
- samples of weapons and laptop computers assigned to ATF 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 October 1, 2002, and August 31, 2007, related to 30 former ATF personnel, to determine if all weapons and laptop computers

were returned. Moreover, we reviewed disposal actions initiated between October 1, 2002, and August 31, 2007, to ensure these actions were adequately supported.

## APPENDIX II

### SAMPLING DESIGN

The ATF database we tested contained 22,476 weapons and 7,505 laptop computers assigned to all ATF offices and officials located around the country and abroad. We selected 16 offices: (1) the Materiel Management Operations Center at Landover Maryland, (2) the ATF Academy at Glynco, Georgia, (3) Martinsburg, West Virginia, (4) Atlanta, Georgia, (5) Kansas City, Kansas, (6) Las Vegas, Nevada, (7) Little Rock, Arkansas, (8) Los Angeles, California, (9) Riverside, California, (10) San Francisco, California, (11) New Orleans, Louisiana, (12) Shreveport, Louisiana, (13) Philadelphia, Pennsylvania, (14) Pittsburgh, Pennsylvania, (15) St. Louis, Missouri, and (16) Washington, D.C.

#### 16 Offices Reviewed July 30, 2007, through April 16, 2008



Source: OIG analysis of ATF data

The red dots represent the cities where we performed testing.



During the preliminary testing phase (Phase I), we conducted a 100-percent review of inventory at the Atlanta and Washington Field Divisions. We tested a total of 853 weapons and 472 laptop computers as shown in the table below.

**Weapons and Laptop Computers Tested**

Location	Weapons	Laptop computers
	Number Tested	Number Tested
Atlanta	331	238
Washington, D.C.	522	234
<b>Total</b>	<b>853</b>	<b>472</b>

Source: ATF's property management system

During the additional testing phase (Phase II), to provide effective coverage and efficient testing of the items, we selected a statistical sample design, as shown in the following table. We tested a total sample of 935 weapons and 560 laptop computers.

**Sample of Weapons and Laptop Computers Tested**

Location	Weapons Tested	Laptop Computers Tested
Glynco	92	69
Landover	0	31
Martinsburg	165	58
Kansas City	58	53
Las Vegas	60	25
Little Rock	36	21
Los Angeles	97	61
Riverside	31	16
San Francisco	64	56
New Orleans	59	37
Shreveport	46	18
Philadelphia	77	48
Pittsburgh	66	35
St. Louis	84	32
<b>Total</b>	<b>935</b>	<b>560</b>

Source: ATF's property management system

## APPENDIX III

### CIRCUMSTANCES OF WEAPON LOSSES REPORTED TO INTERNAL AFFAIRS

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
1 <sup>66</sup>	9/27/2002	Atlanta	Special Agent's private vehicle was burglarized. Weapon stolen from center console. <b>3-day suspension</b>
2	11/13/2002	Phoenix	Special Agent's home was burglarized. The weapon was stolen from underneath a mattress. <b>3-day suspension</b>
3	12/11/2002	Detroit	Special Agent's hotel room was burglarized. Weapon was later recovered. <b>Letter of Clearance</b>
4	12/20/2002	Houston	Special Agent's ATF vehicle was burglarized. <b>3-day suspension</b>
5	4/2003	Atlanta	Special Agent's weapon was discovered missing during an inventory. <b>4-day suspension</b>
6	4/2003	Los Angeles	Special Agent's weapon was discovered missing during an inventory. <b>Letter of Reprimand</b>
7	5/21/2003	San Francisco	Special Agent's private vehicle was burglarized. Weapon was recovered by local law enforcement. <b>4-day suspension</b>
8	6/9/2003	Louisville	Special Agent lost weapon after he forgot he placed it on his vehicle while loading the vehicle. <b>3-day suspension</b>
9	7/26/2003	Grand Rapids	Special Agent initially lost his weapon but later found it under the seat of his ATF vehicle. <b>3-day suspension</b>
10	9/20/2003	Greensboro	Special Agent's hotel room was burglarized. <b>3-day suspension</b>
11	10/13/2003	Chicago	Special Agent's private vehicle was burglarized. <b>3-day suspension</b>
12	11/3/2003	Miami	Special Agent's hotel room was burglarized. <b>3-day suspension</b>

<sup>65</sup> In the Description of Loss column, we added in bold the result of the Office of Professional Responsibility's adjudication of the loss.

<sup>66</sup> While weapon loss 1 occurred prior to our audit period beginning October 1, 2002, we included it in our audit because ATF reported it during the period of our review.

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
13	3/12/2004	Sacramento	Special Agent left the weapon in a gas station bathroom. The agent did not report the item missing and did not immediately retrieve it when it was recovered. <b>4-day suspension</b>
14	3/13/2004	Atlanta	Special Agent left weapon in dressing room of clothing store. The agent did not report the loss. Supervisor learned of loss when local police ran a trace. <b>8-day suspension</b>
15	4/30/2004	San Diego	Special Agent left weapon in athletic bag and forgot. Agent originally thought weapon was stolen from secured briefcase in the trunk of his vehicle. <b>3-day suspension</b>
16	7/8/2004	Washington, D.C.	Weapon believed to have been stolen from a Washington, D.C, sorting facility belonging to a shipping company. Empty, damaged case arrived in Harrisburg, PA. <b>Not Applicable-No Investigation</b>
17	8/13/2004	McAllen	Special Agent's ATF Vehicle was burglarized. Weapon was stolen from under car seat. Later recovered. <b>5-day suspension</b>
18	9/28/2004	Rochester	Weapon was stolen and later recovered during shipment. <b>Not Applicable-No Investigation</b>
19	10/10/2004	New Orleans	Special Agent left weapon in her purse on a shuttle at an airport. Later recovered from airport police. <b>3-day suspension</b>
20	10/12/2004	San Diego	Special Agent's home was burglarized. Lives with another agent who also had weapon stolen. <b>Memorandum of Clearance<sup>67</sup></b>
21	10/12/2004	San Diego	Special Agent's home was burglarized. Lives with another agent who also had weapon stolen. <b>Memorandum of Clearance</b>
22	12/3/2004	Special Response Team	Special Agent's private vehicle was burglarized while agent was moving residence. <b>3-day suspension</b>
23	12/21/2004	St. Louis	Special Agent's private vehicle was burglarized in parking lot during a football game. Weapon was stolen from secured trunk. <b>3-day suspension</b>
24	1/12/2005	Detroit	Special Agent left weapon on an airplane. Later returned to agent by airport authorities. <b>3-day suspension</b>

<sup>67</sup> A Memorandum of Clearance is an action that clears the employee of any wrongdoing and does not result in disciplinary action.

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
25	5/19/2005	Training and Professional Development	Weapon reported missing during an inventory. Weapon recovered from agent recently transferred to Fort Lauderdale, Florida. <b>Not Applicable-No Investigation</b>
26	5/19/2005	Training and Professional Development	Weapon reported missing during an inventory. Weapon recovered from agent recently transferred to Fort Lauderdale, Florida. <b>Not Applicable-No Investigation</b>
27	5/19/2005	Training and Professional Development	Weapon reported missing during an inventory. Weapon recovered in vault, initially overlooked during inventory. <b>Not Applicable-No Investigation</b>
28	5/19/2005	Training and Professional Development	Weapon reported missing during an inventory. Weapon recovered in vault, initially overlooked during inventory. <b>Not Applicable-No Investigation</b>
29	6/19/2005	Dallas	Special Agent left weapon on the hood of a rental truck. <b>3-day suspension</b>
30	6/30/2005	Tulsa	Special Agent's ATF vehicle was burglarized while parked at a hotel. Weapon was stolen from a secured lock box. <b>Memorandum of Clearance</b>
31	7/16/2005	Miami	Special Agent left weapon in fanny pack in a shopping cart at a wholesale store. Weapon was later recovered. <b>3-day suspension</b>
32	9/27/2005	Yakima	Weapon discovered missing from a vault by the primary user. <b>Letter of Caution</b>
33	10/7/2005	Melville	Special Agent left weapon on a chair in a hotel parking garage. <b>3-day suspension</b>
34	12/5/2005	Columbus	Special Agent's undercover vehicle was burglarized during an operation. Weapon stolen from cooler in the vehicle's cab. <b>Not Applicable-No Investigation</b>
35	12/27/2005	Nashville	Special Agent was returned the wrong weapon after testifying in court. Later recovered. <b>Not Applicable-No Investigation</b>
36	1/23/2006	Los Angeles	Prop weapon reported missing during inventory. Recovered from agent's ATF vehicle. <b>Removal</b>
37	2/26/2006	Baltimore	Special Agent's home was burglarized. Weapon stolen from bedroom dresser. Later recovered in a restaurant dumpster. <b>4-day suspension</b>

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
38	3/10/2006	New Orleans	Weapons reported missing during an inventory. Later recovered at the Mandeville field office. <b>Letter of Caution</b>
39	5/21/2006	Miami	Weapons possibly thrown out in the trash along with moving boxes. Second loss of his personal weapon within a 1-year period. <b>10-day suspension</b>
40	7/28/2006	Houston	Special Agent left weapon in restroom stall. Recovered the same day. <b>3-day suspension</b>
41	8/21/2006	Washington	Special Agent's private vehicle was burglarized at residence. Not properly secured in vehicle. Agent (an ASAC) realized car door was ajar on 8/11/2006, but did not check whether any property was missing until 8/21/2006. <b>1-day suspension</b>
42	8/21/2006	Washington	Special Agent's private vehicle was burglarized at residence. Not properly secured in vehicle. Agent (an ASAC) realized car door was ajar on 8/11/2006, but did not check whether any property was missing until 8/21/2006. <b>1-day suspension</b>
43	8/24/2006	Tactical Operations Branch	Special Agent's friend's (also Special Agent) private vehicle was burglarized. <b>1-day suspension</b>
44	8/26/2006	Dallas	Special Agent's ATF vehicle was burglarized at residence. Weapon stolen from a lockbox secured in the vehicle. No signs of forced entry into vehicle. <b>1-day suspension</b>
45	9/5/2006	Detroit	Special Agent's private vehicle was burglarized. Stolen from under the front seat of vehicle. <b>1-day suspension</b>
46	9/19/2006	Washington	Special Agent's private vehicle was burglarized at residence. Agent left the vehicle unlocked with garage door partially open. <b>10-day suspension</b> The agent received a 2-day suspension in 2002 for another lost weapon and a letter of reprimand in 2003 for misusing his official credentials.
47	9/26/2006	Houston	Special Agent's ATF vehicle was burglarized in parking lot. Weapon stolen from secured double locked trunk. Later recovered. <b>Not Applicable-No Investigation</b>
48	10/16/2006	Madison	Special Agent's ATF vehicle was burglarized. Weapon stolen from trunk. <b>Letter of Caution</b>
49	10/21/2006	Houston	Special Agent's ATF vehicle was burglarized in front of residence. <b>Pending 3-day suspension</b>

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
50	10/22/2006	Grand Rapids	Special Agent's private vehicle was burglarized in front of brother's residence. <b>1-day suspension</b>
51	10/28/2006	Denver	Special Agent's ATF vehicle was burglarized in front of residence. <b>Letter of Caution</b>
52	12/14/2006	McAllen	Special Agent's ATF vehicle was burglarized in hotel parking lot. <b>Letter of Caution</b>
53	12/16/2006	Charlotte	Special Agent's private vehicle was burglarized while parked at residence. <b>1-day suspension</b>
54	1/24/2007	Little Rock	Special Agent's home was burglarized. Weapon was stolen from secured cabinet in laundry room. Later recovered. <b>Not Applicable-No Investigation</b>
55	2/26/2007	Houston	Tactical Operation Officer's office was burglarized. <b>Not Applicable-No Investigation</b>
56	3/14/2007	Charleston	Special Agent's home was burglarized. Weapon was stolen from nightstand drawer. <b>Not Applicable-No Investigation</b>
57	3/22/2007	Shreveport	Special Agent lost weapon during a pursuit. <b>Letter of Clearance</b>
58	4/21/2007	Detroit	Special Agent lost weapon in water while fishing. <b>Letter of Clearance</b>
59	6/18/2007	Washington	Special Agent's home was burglarized. Weapon was stolen from nightstand drawer. (Second loss for ASAC; first loss 8/21/2006) <b>Pending as of 11/30/2007</b>
60	6/18/2007	Washington	Special Agent's home was burglarized. Weapon was stolen from nightstand drawer. (Second loss for ASAC; first loss 8/21/2006) <b>Pending as of 11/30/2007</b>
61	6/22/2007	Houston	Special Agent left weapon in briefcase at interviewee's residence. Interviewee contacted the ATF and agent retrieved the weapon. <b>Pending as of 11/15/2007</b>
62	7/10/2007	Fort Worth	Special Agent left weapon in bathroom stall at the field office. <b>Pending as of 11/8/2007</b>
63	7/17/2007	New Orleans	Special Agent's ATF vehicle was burglarized in field office parking deck. <b>Pending as of 11/14/2007</b>

NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN <sup>65</sup>
64 <sup>68</sup>	9/6/2006	Macon	Stolen non-ATF weapons. Two weapons being held as evidence. <b>2-day suspension</b>
65	10/19/2005	Beaumont	Missing non-ATF weapon. Weapon being held as evidence was lost during Hurricane Rita. <b>No disciplinary action</b>

Source: ATF Internal Affairs investigative reports

---

<sup>68</sup> ATF lost items 64 and 65, which were seized weapons, rather than weapons assigned to staff. These items were reported to Internal Affairs. These items also are not included in our analysis of total lost, stolen, or missing ATF weapons.

**APPENDIX IV**

**CIRCUMSTANCES OF LAPTOP COMPUTER LOSSES  
REPORTED TO INTERNAL AFFAIRS**

<b>NO.</b>	<b>LOSS DATE</b>	<b>FIELD OFFICE</b>	<b>DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN</b>	<b>CONTENTS OF LAPTOP ACCORDING TO INVESTIGATIVE REPORT</b>
1 <sup>69</sup>	9/26/2002	ATF headquarters	Stolen from hotel room.	Travel Vouchers, Contractor lists, Physical security surveys.
2	10/16/2002	New York	Stolen from room at the Cardozo School of Law	CND <sup>70</sup>
3	12/13/2002	Miami	Stolen from back seat of private vehicle parked at residence. <b>Letter of Reprimand.</b>	CND
4	12/17/2002	San Francisco	Stolen from briefcase in back seat of private vehicle parked at residence. <b>Letter of Reprimand.</b>	CND
5	1/7/2003	Fayetteville	Special Agent left computer on top of ATF vehicle as he drove away from his residence. <b>Letter of Reprimand.</b>	CND
6	1/27/2003	San Francisco	Stolen from ATF vehicle parked in San Francisco Police Department parking deck.	CND
7	2/11/2003	St. Paul	Stolen from hotel conference room during training course. <b>Memorandum of Clearance.</b>	CND
8	3/16/2003	ATF headquarters	Stolen from employee's residence.	CND
9	8/24/2003	Computer Forensics Branch	Agent transferred and took property with him. Surveillance camera recorded employee taking equipment. Manager could not ensure employee took correct property. Manager notified Internal Affairs. Employee ordered to do an inventory.	CND
10	1/28/2004	Tampa	Stolen from rental vehicle parked at a restaurant.	CND
11	2/3/2004	Explosives Technology Branch, Atlanta	Stolen from private vehicle parked at hotel parking lot.	CND

<sup>69</sup> Although this laptop computer was stolen September 26, 2002, we included it in our audit period beginning October 1, 2002.

<sup>70</sup> ATF could not determine (CND) the contents of the laptop computer.



NO.	LOSS DATE	FIELD OFFICE	DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN	CONTENTS OF LAPTOP ACCORDING TO INVESTIGATIVE REPORT
12	6/21/2004	Savannah	Stolen from ATF vehicle parked at residence.	CND
13	9/16/2004	Nashville	Stolen from Special Agent's ATF vehicle. <b>Pending.</b>	CND
14	10/12/2004	Boston	Stolen from Special Agent's ATF vehicle.	CND
15	11/28/2004	Boston	Stolen from Special Agent's private vehicle	CND
16	3/27/2005	Boston	Stolen from Special Agent's ATF vehicle parked at residence.	CND
17	6/25/2005	Washington	Stolen from Special Agent's workstation.	CND
18	9/10/2005	Los Angeles	Contractor's laptop stolen from private vehicle parked at residence.	CND
19	9/14/2005	Detroit	Item unaccounted for during inventory, Item located at residence.	CND
20	9/14/2005	Detroit	Item unaccounted for during inventory. Agent had no recollection of having item.	CND
21	9/14/2005	Detroit	Item unaccounted for during inventory. Item assigned to another agent.	CND
22	1/9/2006	San Francisco	Stolen from ATF vehicle parked in restaurant parking lot.	CND
23	2/24/2006	Boston	Stolen from private vehicle parked at firearm licensee.	CND
24	2/26/2006	Houston	Stolen from Tactical Operations Office. The next four laptop computers were also stolen in this same incident.	CND
25	2/26/2006	Houston	Stolen from Tactical Operations Office.	CND
26	2/26/2006	Houston	Stolen from Tactical Operations Office.	CND
27	2/26/2006	Houston	Stolen from Tactical Operations Office.	CND
28	2/26/2006	Houston	Stolen from Tactical Operations Office.	CND
29	3/7/2006	Nashville	Stolen from ATF vehicle parked at hotel parking lot. The next laptop computer was also stolen in this same incident.	Non-network, configured for vehicle tracking.
30	3/7/2006	Nashville	Stolen from ATF vehicle parked at hotel parking lot.	Non-network, configured for vehicle tracking.
31	3/31/2006	Seattle	Stolen from undercover storefront operation.	Determined value of items purchased and sold.
32	4/2/2006	Los Angeles	Stolen from private vehicle parked overnight at residence. Locked inside trunk.	Agent said it contained sensitive explosives licensee information.

<b>NO.</b>	<b>LOSS DATE</b>	<b>FIELD OFFICE</b>	<b>DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN</b>	<b>CONTENTS OF LAPTOP ACCORDING TO INVESTIGATIVE REPORT</b>
33	4/13/2006	Office of Science and Technology	Stolen from hotel room.	CND
34	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006. The next 5 laptop computers were also stolen in this same incident.	CND
35	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006.	CND
36	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006.	CND
37	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006.	CND
38	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006.	CND
39	9/15/2006	Philadelphia	Stolen from Division office, recovered 9/22/2006.	CND
40	9/28/2006	Detroit	Stolen from ATF vehicle. Rear window was broken.	Personal and work-related information.
41	10/12/2006	Fort Lauderdale	Stolen from ATF vehicle parked at residence.	Hard drive was 2-weeks old. No PII. Password protected.
42	11/1/2006	Office of Science and Technology	Stolen from office credenza.	Employee evaluations.
43	2/27/2007	Financial Investigations Service Division	Stolen from rental vehicle in restaurant parking lot.	E-mails, active case information, personal identifiers for ATF personnel, copies of administrative reports.
44	2/27/2007	Financial Investigations Service Division	Stolen from rental vehicle in restaurant parking lot.	E-mails, personal identifiers for ATF personnel; other personal identifiers, including social security numbers for targets or victims of ATF investigations; user passwords on an Excel spreadsheet.
45	3/14/2007	Charleston	Stolen from Special Agent's residence during burglary.	CND
46	6/9/2007	Computer Forensics Branch	Stolen under other circumstances that were not explained.	Names and addresses of ATF computer forensic examiners.

<b>NO.</b>	<b>LOSS DATE</b>	<b>FIELD OFFICE</b>	<b>DESCRIPTION OF LOSS AND ANY DISCIPLINARY ACTION TAKEN</b>	<b>CONTENTS OF LAPTOP ACCORDING TO INVESTIGATIVE REPORT</b>
47	6/23/2007	ATF headquarters	Left on METRO train. Recovered and returned to employee on 6/25/2007.	CND
48	6/24/2007	San Diego	Stolen from hotel room during conference.	Conference attendee list with phone numbers in computer bag. Encryption software was not installed.
49	7/16/2007	Harrisburg	Stolen from under rear seat in private vehicle.	Printouts with dates of birth and social security numbers for three firearm licensees in computer bag.
50	CND	Computer Forensics Branch	Lost at the Sony service department after ATF shipped it for repair.	Computer wiped clean.
51	CND	Boston	Notation on inventory that item was transferred to Training and Professional Development, Arson Training Branch (ATB), 1851.1 on file. However, ATB does not have it. ATB says it could have been sent to ATF National Academy to be used in burn cells to demonstrate survivability of hard drives in a fire environment.	CND
52	CND	Boston	Lost during shipping during agency computer refresh. The agent opened an empty box. The next laptop computer was also lost in this same incident.	CND
53	CND	Boston	Lost during shipping during agency computer refresh. The agent opened an empty box.	CND

Source: ATF Internal Affairs investigative reports

**APPENDIX V**

**ANALYSIS OF LOST, STOLEN, OR MISSING WEAPONS  
REPORTED TO INTERNAL AFFAIRS**

<b>NUMBER</b>	<b>LOSS TYPE</b>	<b>DAYS BETWEEN LOSS AND REPORTED DATES</b>	<b>REPORTED TIMELY<sup>71</sup></b>
1	Stolen	0	Yes
2	Stolen	2	No
3	Stolen	0	Yes
4	Stolen	0	Yes
5	Lost	CND <sup>72</sup>	CND
6	Lost	CND	CND
7	Stolen	0	Yes
8	Lost	0	Yes
9	Lost	2	No
10	Stolen	3	No
11	Stolen	0	Yes
12	Stolen	0	Yes
13	Lost	0	Yes
14	Lost	19	No
15	Lost	0	Yes
16	Lost	1	Yes
17	Stolen	0	Yes
18	Lost	0	Yes
19	Lost	0	Yes
20	Stolen	0	Yes
21	Stolen	0	Yes
22	Stolen	0	Yes
23	Stolen	0	Yes
24	Lost	0	Yes
25	Lost	0	Yes
26	Lost	0	Yes
27	Lost	0	Yes
28	Lost	0	Yes
29	Lost	0	Yes
30	Stolen	0	Yes
31	Lost	1	Yes
32	Lost	1	Yes
33	Stolen	0	Yes

<sup>71</sup> ATF required that its employees report a loss immediately to a SAC, division director, or chief. We considered any loss reported 2 or more days after the loss occurred as not reported in a timely manner.

<sup>72</sup> We could not determine (CND) how quickly some losses were reported because the investigative report did not include the date of the loss, the date the loss was reported, or both.

<b>NUMBER</b>	<b>LOSS TYPE</b>	<b>DAYS BETWEEN LOSS AND REPORTED DATES</b>	<b>REPORTED TIMELY<sup>71</sup></b>
34	Lost	0	Yes
35	Stolen	0	Yes
36	Lost	0	Yes
37	Lost	1	Yes
38	Stolen	0	Yes
39	Lost	0	Yes
40	Lost	0	Yes
41	Lost	0	Yes
42	Stolen	1	Yes
43	Stolen	1	Yes
44	Stolen	0	Yes
45	Stolen	0	Yes
46	Stolen	0	Yes
47	Stolen	0	Yes
48	Stolen	0	Yes
49	Stolen	0	Yes
50	Stolen	0	Yes
51	Stolen	0	Yes
52	Stolen	0	Yes
53	Stolen	0	Yes
54	Stolen	0	Yes
55	Stolen	0	Yes
56	Stolen	1	Yes
57	Stolen	0	Yes
58	Lost	1	Yes
59	Lost	0	Yes
60	Stolen	0	Yes
61	Stolen	0	Yes
62	Lost	0	Yes
63	Lost	0	Yes
64	Stolen	0	Yes

Source: ATF Internal Affairs investigative reports

**APPENDIX VI**

**ANALYSIS OF LOST, STOLEN, OR MISSING LAPTOP COMPUTERS  
REPORTED TO INTERNAL AFFAIRS**

<b>NUMBER</b>	<b>LOSS TYPE</b>	<b>DAYS BETWEEN LOSS AND REPORTED DATES</b>	<b>REPORTED TIMELY<sup>73</sup></b>	<b>CONTAINED SENSITIVE/ CLASSIFIED INFORMATION</b>	<b>REPORTED TO DOJ</b>
1	Stolen	0	Yes	No	No
2	Stolen	CND	CND	CND	No
3	Stolen	0	Yes	CND	No
4	Stolen	0	Yes	CND	No
5	Lost	0	Yes	CND	No
6	Stolen	0	Yes	CND	No
7	Stolen	0	Yes	CND	No
8	Stolen	1	Yes	No	No
9	Stolen	1	Yes	CND	No
10	Stolen	0	Yes	CND	No
11	Stolen	0	Yes	CND	No
12	Stolen	0	Yes	CND	No
13	Stolen	0	Yes	CND	No
14	Stolen	1	Yes	No	No
15	Stolen	1	Yes	No	No
16	Stolen	0	Yes	No	No
17	Stolen	CND	CND	Yes	No
18	Stolen	CND	CND	CND	No
19	Lost	0	Yes	CND	No
20	Lost	0	Yes	CND	No
21	Lost	0	Yes	CND	No
22	Stolen	0	Yes	CND	No
23	Stolen	0	Yes	CND	No
24	Stolen	1	Yes	CND	No
25	Stolen	1	Yes	CND	No
26	Stolen	1	Yes	CND	No
27	Stolen	1	Yes	CND	No
28	Stolen	1	Yes	CND	No
29	Stolen	0	Yes	No	No
30	Stolen	0	Yes	No	No
31	Stolen	0	Yes	No	No
32	Stolen	0	Yes	Yes	No
33	Stolen	0	Yes	CND	No
34	Stolen	0	Yes	CND	No
35	Stolen	0	Yes	CND	No
36	Stolen	0	Yes	CND	No
37	Stolen	0	Yes	CND	No
38	Stolen	0	Yes	CND	No
39	Stolen	0	Yes	CND	No
40	Stolen	0	Yes	Yes	No
41	Stolen	0	Yes	CND	No

<b>NUMBER</b>	<b>LOSS TYPE</b>	<b>DAYS BETWEEN LOSS AND REPORTED DATES</b>	<b>REPORTED TIMELY<sup>73</sup></b>	<b>CONTAINED SENSITIVE/ CLASSIFIED INFORMATION</b>	<b>REPORTED TO DOJ</b>
42	Stolen	0	Yes	<b>Yes</b>	<b>No</b>
43	Stolen	0	Yes	<b>Yes</b>	<b>No</b>
44	Stolen	0	Yes	<b>Yes</b>	<b>No</b>
45	Stolen	0	Yes	No	<b>No</b>
46	Stolen	0	Yes	<b>Yes</b>	<b>No</b>
47	Stolen	0	Yes	No	<b>No</b>
48	Stolen	0	Yes	No	<b>No</b>
49	Lost	0	Yes	No	<b>No</b>
50	Lost	<b>CND</b>	<b>CND</b>	No	<b>No</b>
51	Lost	<b>CND</b>	<b>CND</b>	<b>CND</b>	<b>No</b>
52	Lost	<b>CND</b>	<b>CND</b>	<b>CND</b>	<b>No</b>
53	Lost	<b>CND</b>	<b>CND</b>	<b>CND</b>	<b>No</b>

Source: ATF Internal Affairs investigative reports

**APPENDIX VII**

**ANALYSIS OF PROPERTY MANAGEMENT RECORDS**

**Table 1: ATF UNIVERSE OF WEAPONS**

<b>Field Name</b>	<b>Data Type</b>	<b>Number of records where field name contained data</b>	<b>Number of records where field name was blank</b>	<b>Total</b>
PIN	Property Identification Number	22,476	0	22,476
STEWARD/ORG	Code Numbers and Location Names	22,476	0	22,476
SERIAL NUMBER	Serial number	22,358	118	22,476
MANUFACTURER	Manufacturer Name	22,476	0	22,476
MODEL	Model number	22,476	0	22,476
ASSET TYPE	Property Description	22,476	0	22,476
USER	Person Assigned	15,637	6,839 <sup>73</sup>	22,476

Source: ATF property management system

**Table 2: ATF UNIVERSE OF LAPTOP COMPUTERS**

<b>Field Name</b>	<b>Data Type</b>	<b>Number of records where field name contained data</b>	<b>Number of records where field name was blank</b>	<b>Total</b>
PIN	Property Identification Number	7,505	0	7,505
STEWARD/ORG	Code Numbers and Location Names	7,505	0	7,505
SERIAL NUMBER	Serial number	7,503	2	7,505
MANUFACTURER	Manufacturer Name	7,505	0	7,505
MODEL	Model number	7,505	0	7,505
ASSET TYPE	Property Description	7,505	0	7,505
USER	Person Assigned	5,888	1,617	7,505

Source: ATF property management system

<sup>73</sup> The weapons that were not assigned to individuals were either vault weapons or training weapons for which all had a Steward/Org assigned.



**APPENDIX VIII**

**LOST, STOLEN, OR MISSING WEAPONS AND LAPTOP COMPUTERS  
REPORTED TO INTERNAL AFFAIRS BY ATF FIELD OFFICE**

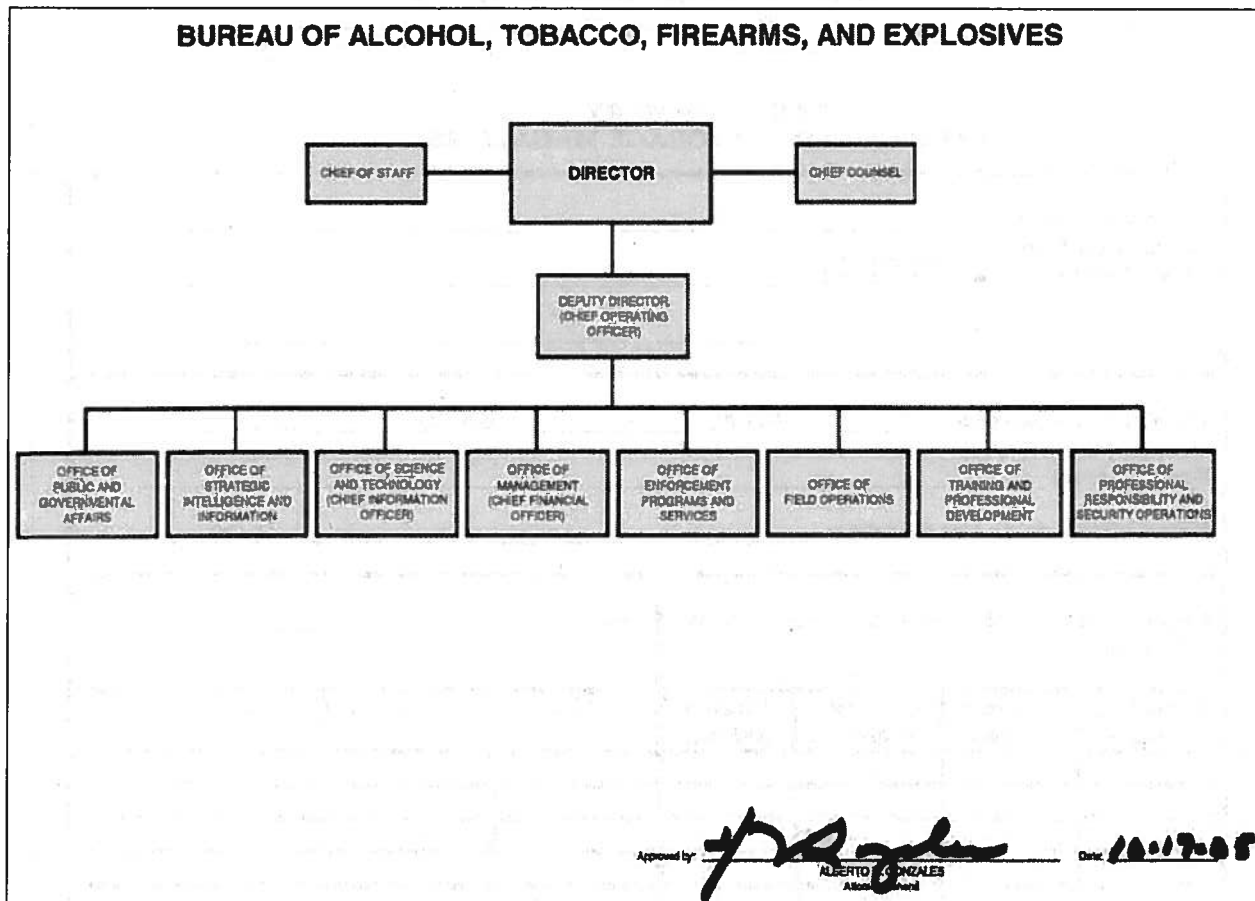
<b>FIELD OFFICE</b>	<b>WEAPONS</b>	<b>LAPTOP COMPUTERS</b>
Atlanta, GA	3	1
Baltimore, MD	1	0
Boston, MA	0	7
Charleston, SC	1	1
Charlotte, NC	1	0
Chicago, IL	1	0
Columbus, OH	1	0
Dallas, TX	2	0
Denver, CO	1	0
Detroit, MI	4	4
Fayetteville, AR	0	1
Fort Lauderdale, FL	0	1
Fort Worth, TX	1	0
Grand Rapids, MI	2	0
Greensboro, NC	1	0
Headquarters	7	10
Harrisburg, PA	0	1
Houston, TX	6	5
Little Rock, AR	1	0
Los Angeles, CA	2	2
Louisville, KY	1	0
Madison, WI	1	0
McAllen, TX	2	0
Melville, NY	1	0
Miami, FL	3	1
Nashville, TN	1	3
New Orleans, LA	3	0
New York, NY	0	1
Philadelphia, PA	0	6
Phoenix, AZ	1	0
Rochester, NY	1	0
Sacramento, CA	1	0
San Diego, CA	3	1
San Francisco, CA	1	3
Savannah, GA	0	1
Seattle, WA	0	1
Shreveport, LA	1	0
St. Louis, MO	1	0
St. Paul, MN	0	1
Tampa, FL	0	1
Tulsa, OK	1	0
Yakima, WA	1	0
Washington, D.C.	5	1
<b>TOTAL</b>	<b>63</b>	<b>53</b>

Source: ATF Internal Affairs investigative reports





ORGANIZATIONAL CHART



Source: ATF website

ATF FORM 1851.3, REPORT OF SURVEY

U.S. Department of Justice  
Bureau of Alcohol, Tobacco, Firearms and Explosives

Report of Survey

NCIC Report Number: \_\_\_\_\_

To: \_\_\_\_\_

From: \_\_\_\_\_

Organization Code	Item Description <i>(include manufacturer and model no.)</i>	PIN	Serial Number	Quantity	Acquisition Cost		Current Value		
					Dollars	Cents	Dollars	Cents	
<b>Current Market Value: Grand Total</b>									

Circumstances:

Stolen  Damaged  Destroyed  Lost  Other (specify)  \_\_\_\_\_

During an extensive inventory process, the items on the attached excel spreadsheet could not be located for the St Paul Field Division

No Further Action Required

Forward for Additional Review

Signature of Accountable Officer \_\_\_\_\_

Report of Survey No. \_\_\_\_\_

ROS Initiator \_\_\_\_\_

Date \_\_\_\_\_

ATF Form 1851.3  
Revised June 2007

Source: ATF Materiel Management Branch

## APPENDIX XIII

### ACRONYMS AND ABBREVIATIONS

<b>ATF</b>	Bureau of Alcohol, Tobacco, Firearms and Explosives
<b>CIO</b>	Chief Information Officer
<b>DEA</b>	Drug Enforcement Administration
<b>DOJ</b>	Department of Justice
<b>DOJCERT</b>	Department of Justice Computer Emergency Response Team
<b>FBI</b>	Federal Bureau of Investigation
<b>NCIC</b>	National Crime Information Center
<b>NSI</b>	National Security Information
<b>OIG</b>	Office of the Inspector General
<b>OMB</b>	Office of Management and Budget
<b>OPRSO</b>	Office of Professional Responsibility and Security Operations
<b>OST</b>	Office of Science and Technology
<b>POV</b>	Privately-owned vehicle

## APPENDIX XIV

# THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES' RESPONSE TO THE DRAFT AUDIT REPORT



U.S. Department of Justice

Bureau of Alcohol, Tobacco,  
Firearms and Explosives

*Office of the Director*

SEP 10 2008

Washington, DC 20226

MEMORANDUM TO: Assistant Inspector General for Audit  
Office of the Inspector General

FROM: Acting Director

SUBJECT: Response to the Office of Inspector General's Draft Audit Report on  
the Bureau of Alcohol, Tobacco, Firearms and Explosives Controls  
Over Its Weapons, Laptop Computers and Other Sensitive Property

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) appreciates the opportunity to respond to the Office of Inspector General's (OIG) findings and recommendations on the draft audit report entitled "The Bureau of Alcohol, Tobacco, Firearms and Explosives' Controls Over Its Weapons, Laptop Computers and Other Sensitive Property." ATF is committed to strengthening its controls over the loss and theft of weapons and laptop computers.

ATF has reviewed the OIG's draft report and this memorandum will convey ATF's response to each of the recommendations. With respect to most of the recommendations, ATF agrees or partially agrees with the recommendations. ATF disagrees with one recommendation. In the instances where ATF disagrees or partially agrees, ATF has outlined the policies and procedures that currently exist that address the concerns raised by the OIG. ATF has also addressed the specific actions ATF will take to increase awareness of those policies and procedures, and to ensure that employees comply with those policies and procedures.

We are revising our procedures of reporting losses of weapons or laptops. Effective September 30, 2008, ATF will require all losses of weapons or laptops to be reported to the ATF Joint Support Operations Center (JSOC). The JSOC is a 24-hour operation, and the employees who staff the JSOC will be assigned the following responsibilities: 1) ensure the timely documentation of the loss of weapons and laptop computers; 2) ensure the timely reporting of the loss of a laptop computer to the Department of Justice Computer Emergency Response Team (DOJCERT), and 3) ensure the timely entry of the loss of a laptop computer or weapon into the National Crime Information Center's (NCIC) database.

ATF's Deputy Director will also issue a memorandum to all employees to remind them of their responsibility to account for weapons, laptops, ammunition, and explosives. This memorandum will also address the importance of reporting losses in a timely manner.

Assistant Inspector General for Audit

ATF's respective responses to the OIG's recommendations are set forth below:

**Recommendation Number 1: Ensure that ATF staff notifies the Materiel Management Branch of all weapon and laptop computer losses and maintain copies of all supporting documentation.**

**ATF's Response:** ATF agrees with this recommendation. ATF currently has reporting procedures in place that address the reporting of lost or stolen weapons and laptops. The notification procedures are outlined in ATF Order 1850.2D, Personal Property Management Program, dated April 29, 2008, Chapter E, Paragraph 72 and 73. ATF recognizes that we need to implement measures to ensure that the provisions of the order are followed by each ATF employee.

ATF recognizes the need for a more reliable and comprehensive reporting method for sensitive items that have a short reporting deadline. Accordingly, ATF is revising its current reporting procedures to include simultaneous electronic notification to the Internal Affairs Division (IAD), the Materiel Management Branch (MMB), the ATF JSOC, and the Information Services Division (ISD) (information technology assets) when accountable property is lost or stolen. ATF believes these additional steps will strengthen its existing procedures to ensure the timely reporting, and ensuring the MMB is timely notified. This revised procedure will be in effect no later than September 30, 2008.

ATF recognizes the need to reinforce the importance of the reporting process. ATF's Deputy Director will issue a memorandum to all employees which will accomplish the following four tasks: 1) reference ATF Order 1850.2D; 2) underscore their responsibility to account for weapons, laptops, ammunition and explosives; 3) initiate the new form and electronic reporting process; and 4) summarize the deadlines relative to the timely reporting of such losses.

**Recommendation Number 2: Ensure that for each loss Materiel Management provides Internal Affairs with the Report of Survey and information needed to conduct an investigation.**

**ATF's Response:** ATF agrees with this recommendation. ATF's current procedure requires the MMB to initiate a Report of Survey (ROS) within 3 working days of notification of any loss or theft. A copy of the ROS is provided to the IAD. The ROS includes all of the pertinent information relating to the loss or theft to include a copy of the electronic notification, copies of any police report, and any other pertinent documentation. The notification procedures are outlined in ATF Order 1850.2D, of the Property Management Program, dated April 29, 2008, Chapter E, Paragraph 72 and 73.



Assistant Inspector General for Audit

ATF is aware that the OIG auditors found instances of losses or thefts of weapons and laptops that were not reported to the IAD. ATF is revising its current reporting procedures contained in ATF Property Management Order 1850.2D to include simultaneous electronic notification to the IAD, MMB, ATF JSOC and ISD (information technology assets) when accountable property is lost or stolen. ATF believes these additional steps will strengthen its existing procedures to ensure the timely reporting, and to ensure the MMB is timely notified. This revised procedure will be in effect no later than September 30, 2008.

**Recommendation Number 3. Implement a written policy for reporting losses of ammunition to Internal Affairs for investigation.**

**ATF's Response:** ATF agrees with this recommendation. ATF's current procedures, contained in ATF Personal Property Management Order 1850.2D, dated April 29, 2008, require any incident involving a break-in or theft from an ammunition storage facility to be immediately reported by the ATF Division Chief or Special Agent in Charge to the IAD. The audit revealed that ATF is in fact complying with reporting such incidents, and found that disciplinary actions were taken where the instance involved employee misconduct.

ATF is revising its current procedures to require the simultaneous electronic reporting of any lost or stolen ammunition to the IAD, MMB, and ATF JSOC. In addition to revising its ATF Personal Property Management Order 1850.2D, dated April 29, 2008, all ATF offices will complete a 100 percent ammunition inventory by October 15, 2008, to establish a supported baseline for future perpetual inventories. The MMB will provide instructions to all offices for this inventory no later than September 15, 2008. ATF believes these additional steps will strengthen its existing procedures relative to reporting losses of ammunition.

**Recommendation Number 4. Implement procedures to determine the contents of lost, stolen, and or missing laptop computers, specifically:**

- a) Whether the laptop computer contained classified information;
- b) Whether the laptop computer contained sensitive or personally identifiable information; and
- c) Whether the lost, stolen, or missing laptop computer was protected with encryption software.

**ATF's Response:** ATF agrees with this recommendation. ATF currently has a procedure in place that requires ATF employees to provide complete, accurate and timely incident reports summarizing the loss of ATF laptop computers. These reports require an assessment of what type of information was on the system or device; whether the system or device contained sensitive or personally identifiable information (PII), and whether or not the system or device was encrypted. These reports are currently submitted to the ATF Help Desk and subsequently

Assistant Inspector General for Audit

reported to the DOJCERT. These procedures are available to all ATF employees through the ATF Intra-web. These current procedures are contained in a Chief Information Officer (CIO) letter dated, March 2007.

ATF is aware that the OIG auditors found instances, whereby ATF was not accurately capturing the contents of lost, missing, or stolen laptops. ATF is revising its current procedures to allow for electronic reporting of laptops and weapons to the ATF JSOC. The JSOC is a 24-hour operation that will be the Bureau's component responsible for ensuring that all lost or stolen laptops and weapons are immediately recorded in NCIC and reported to DOJCERT. ATF believes these additional steps will strengthen its existing procedures and ensure the timely reporting and determination of the contents of lost, stolen or missing laptop computers. This revised procedure will be effective no later than September 30, 2008. ATF's Deputy Director will issue a memorandum to all employees emphasizing the new reporting procedure and the importance of meeting the reporting deadlines.

ATF is especially sensitive to the risks that may occur when there is a data breach. ATF has implemented a Data Breach Notification Technical Working Group composed of members from multiple ATF directorates. The working group actually assesses the losses and risks associated with any PII. It then reports to DOJ on the information lost and the procedures being undertaken to remedy the loss. ATF issued data breach notification procedures on August 5, 2008.

**Recommendation Number 5. Require that lost, stolen, or missing weapons and laptop computers are appropriately entered into NCIC.**

**ATF's Response:** ATF partially agrees with this recommendation. ATF recognizes some inconsistencies in our methodology of reporting weapon and laptop losses to NCIC however; losses are reported to the ATF IAD. The current ATF policy requires all incidents involving sensitive items i.e., laptop computers, firearms or capitalized property to be reported within 24 hours. Losses involving firearms or equipment containing classified information must also be reported to the NCIC and local law enforcement officials within 24 hours of discovery. Occasionally a misplaced weapon or laptop will be found shortly after the initial report to IAD, therefore negating the need for further reporting to NCIC. ATF believes this has contributed to some of the findings during the current review.

ATF's revised reporting procedures will rely on the JSOC to be the responsible component for ensuring all lost or stolen laptops and weapons are timely recorded in NCIC and reported to the DOJCERT. Since the JSOC is a 24-hour operation, we believe that this component is best suited to meet these short reporting deadlines. This revised procedure will be effective no later than September 30, 2008. ATF's Deputy Director will issue a memorandum to all employees emphasizing the new reporting procedure and the importance of meeting the reporting deadlines.

Assistant Inspector General for Audit

**Recommendation Number 6: Develop procedures for updating the property management system to ensure accurate and complete weapons and laptop computer records are maintained.**

**ATF's Response:** ATF disagrees with this recommendation because ATF currently has procedures as outlined below. However, ATF acknowledges that enforcement of the use of the Property Management System (Sunflower) and training for those who are responsible for data entry, is necessary.

Property Custodians are designated in writing by the Property Management Representative and have Sunflower access capabilities that allow them to update user information, process reports, and to initiate and accept transactions involving the transfer of assets between organizational elements. E-mail alert notifications are also a function within Sunflower. This system is used to alert managers when a transaction is awaiting action, or an action has occurred affecting the on-hand balance of their account. The electronic transfers are permanently recorded in the system and provide an automated record of the movement of the property. In addition, the permanent edit history files within the Sunflower Property Management System provide a complete history of all transactions affecting an item from the time it is acquired through disposal. Sunflower is an accredited asset management system that provides an electronic audit trail of all transactions affecting an inventory balance.

Source documentation to support the addition or removal of property assets is provided by Property Management Representatives and Property Custodians to the Property Accountable Officer, and is retained on file for three years in accordance with ATF Order 1345.1, Records Management Program, General Records Control Schedule and 44 U.S.C. Chapter 31. The Sunflower Property Management System provides the ability to track assets from cradle to grave and provides time stamp information for each transaction that is posted to an asset, including the date and name of the individual performing the transaction.

Again, all of the procedures outlined above are in ATF Property Management Order 1850.2D. We will ensure that the memorandum that the ATF Deputy Director sends to all employees includes a reminder to input, update and maintain accurate property accountability information in Sunflower. ATF's Office of Management and Office of Training and Professional Development will develop and implement standardized, on-line training of the Sunflower system. Finally, ATF will ensure that property custodians are designated, at a minimum, at the level of branch or field office. A fuller contingent of property custodians will enhance ATF's ability to manage property and ensure accurate and complete computer records. ATF's property management order will be revised to reflect this minimum level of property custodian coverage.

Assistant Inspector General for Audit

**Recommendation Number 7. Locate or report as missing all sampled items not found during the audit.**

**ATF's Response:** ATF partially agrees with this recommendation. The OIG audit covered a 9-month period, during which time some of the sample items were unavailable for physical inspection due to the employee's unavailability, due to training, or another assignment. Those items not physically inspected were characterized as lost by the audit team. Subsequently to that, ATF employees participated in an exhaustive effort with the audit team in faxing laptop verification certificates to the Atlanta Regional Audit Office. We feel that some of these verification certificates were not received or accepted by the audit staff. Furthermore, ATF offers the following for your consideration regarding the high number of discrepancies identified with the information technology equipment.

In 2004, ATF conducted a major Enterprise System Architecture (ESA) Equipment Refresh that included the exchange of all ATF Government Furnished Computer Equipment for leased equipment under the Seat Management Initiative. This refresh involved approximately 4,600 replacement assets located in 256 different locations throughout the United States, Puerto Rico, and the Virgin Islands. In 2006, at the conclusion of the exchange and donation of the government owned computers, ATF conducted a complete inventory. The 100 percent physical inventory identified 274 laptops, 66 percent of the lost items identified in the audit report as lost or missing. ATF initiated a ROS at the conclusion of the reconciliation period in accordance with the procedures outlined in the DOJ policy Bulletin No.05-02. The ROS process required a full review of our records and revealed paperwork postings errors and loss of paperwork.

ATF recognizes the importance of maintaining accountability of computer assets during these wholesale exchanges under the ESA refresh concept. ATF is revising its procedures and will appoint an additional Contracting Officers Technical Representative (COTR) to the seat management contract from the Materiel Management Branch by September 15, 2008. The COTR will have the responsibility of providing oversight and conducting compliance reviews of the Asset Management function of the ESA contract. ATF's Chief Procurement Officer will establish a Contract Management Council consisting of ATF and EDS contract employees. The Council will meet weekly to address contract related challenges, and specifically those associated with Asset Management. The ATF CIO and ATF Chief Financial Officer will be briefed on the results of these meetings and contract compliance reviews on a weekly basis, beginning September 30, 2008.

**Recommendation Number 8. Ensure all laptop computers are encrypted.**

**ATF's Response:** ATF agrees with this recommendation. There are currently 5,848 laptop computers on the ATF network. Since August 20, 2008, the encryption software, Point-Sec, has

Assistant Inspector General for Audit

been installed on 5,810 of these laptops. ATF is currently validating the remaining 38 laptops and their respective user accounts have been disabled until the encryption software is installed. ATF anticipates this will be completed no later than September 30, 2008.

**Recommendation Number 9. Ensure complete, accurate, and timely reports are submitted to the DOJ CIO containing all appropriate ATF laptop computers authorized to process classified information.**

**ATF's Response:** ATF agrees with this recommendation. ATF did provide reports to the DOJ CIO in Fiscal Year 2007 and Fiscal Year 2008; however six of the laptops were omitted from the 2008 report. ATF will review its procedures to determine how this omission occurred and make the necessary adjustment to prevent future occurrences.

**Recommendation Number 10. Ensure complete, accurate, and timely semiannual reports identifying lost, stolen, or missing weapons and laptop computers are submitted to the DOJ Security Officer and Justice Management Division.**

**ATF's Response:** ATF agrees with this recommendation. ATF recently modified the Sunflower Property Management System to provide an automated collection process of all data relating to the loss, damage, or theft of property assets. We are currently finalizing the semiannual Lost, Damage, and or Destroyed report for submission to DOJ, which is due on September 19, 2008.

**Recommendation Number 11. Develop procedures to ensure ATF completes, accurate, and timely incident reports summarizing the loss of ATF laptop computers and submits those reports to DOJCERT, as required by DOJ policy.**

**ATF's Response:** ATF agrees with this recommendation. ATF currently has a procedure in place that requires ATF employees to provide complete, accurate and timely incident reports summarizing the losses of ATF laptop computers. These reports are currently submitted to the ATF Computer Help Desk and subsequently reported to the DOJCERT. These procedures are available to all ATF employees through the ATF Intra-web. These current procedures were reemphasized to all employees through an ATF CIO letter dated March 2007.

ATF is currently revising its procedures to allow for electronic reporting of laptops and weapons to the ATF JSOC. The JSOC is a 24-hour operation that will be ATF's responsible component for ensuring all lost or stolen laptops and weapons are timely recorded in NCIC and reported to DOJCERT. This revised procedure will be effective no later than September 30, 2008.

Assistant Inspector General for Audit

**Recommendation Number 12. Maintain documentation for all disposed property, document data clearing of disposed laptop computers, and update active and disposed property records, as necessary.**

**ATF's Response:** ATF partially agrees with this recommendation. The OIG audit period covered 59 months. ATF did not retain some of the records as prescribed by the following regulations. ATF retains and timely destroys records in accordance with ATF Order 1345.1, Records Management Program, General Records Control Schedule and 44 U.S.C. Chapters 31 and 36 CFR, Subchapter B (Records Management). Additionally, ATF notes that some of the survey reports that were destroyed pertained to property that was lost prior to the 2002 through 2006 timeframe covered by the OIG audit.


**Recommendation Number 13. Develop procedures and maintain documentation to ensure that separated employees return all weapons, laptop computers, and other accountable property before they separate from ATF.**

**ATF's Response:** ATF agrees with this recommendation. ATF Order 2391.1 Employee Clearance Procedures notes that employees must return all ATF property before they separate from ATF. Completed Separation Checklists (ATF Form 2391.1) are forwarded to, and maintained by, the Payroll Processing and Operations Branch (PPOB) in the Human Resources Division. The Separation Checklist forms are maintained separately within PPOB in alphabetical order according to last name. Separated employees have not left ATF with sensitive property. However, we agree that our documentation process needs improvement. We are reviewing our internal control process to ensure the returns of property by employees will be documented by their supervisors and timely entered into Sunflower.

**Recommendation Number 14. Enforce current requirements to perform annual inventories of ammunition and maintain a perpetual inventory system at all ammunition storage locations to ensure accurate and complete records.**

**ATF's Response:** ATF agrees with this recommendation. ATF will conduct an inventory of all ammunition by October 15, 2008. The MMB will provide instructions to all offices for this inventory no later than September 10, 2008. Additionally, effective Fiscal Year 2009, the Office of Inspection will add the inspection of ammunition control logs to its office review process.

Thank you for the opportunity to provide comments to the report. If you would like more information, please contact Acting Assistant Director Kenneth Massey at 202- 648-7500.

  
Michael J. Sullivan

**OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF  
ACTIONS NECESSARY TO CLOSE THE REPORT**

We provided the draft report to ATF for review and requested written comments. ATF's written response is included as Appendix XIV of this report. ATF stated that it agreed with 10 of our recommendations, partially agreed with 3 recommendations, and disagreed with 1 recommendation. All of the recommendations are resolved because ATF either agreed with the recommendations or, for the one recommendation with which it disagreed, proposed sufficient corrective action to address the recommendation. We provide below our analysis of ATF's response to the recommendations. Based on discussions with the ATF staff after the issuance of our draft report, we have made minor technical revisions to the final report. These revisions have no material effect on our results.

1. **Resolved.** We recommended that ATF ensure that its staff notifies the Materiel Management Branch of all weapon and laptop computer losses and maintains copies of all supporting documentation. This recommendation is resolved based on ATF's agreement and its plan to notify the Internal Affairs Division (IAD), Materiel Management Branch (MMB), and the ATF Joint Support Operations Center (JSOC) when accountable property is lost or stolen. However, it is not clear to us how the planned corrective action will both require and verify the proper reporting of these items to IAD, MMB, and JSOC. It is also not clear whether the planned corrective action will include accountable property identified as missing during periodic inventories, as we believe it should.

Given that the corrective action plan requires staff to report each loss to three separate entities, ATF may choose to consider having its staff report these incidents only to the JSOC with the JSOC then reporting the incidents to IAD, MMB, the Department of Justice Computer Emergency Response Team (DOJCERT), and the National Crime Information Center (NCIC), if appropriate. This approach would simplify reporting for the staff and allow the JSOC to ensure that all other reports are properly made. It also has the potential to simplify the corrective actions proposed for Recommendations 2, 3, and 11.

This recommendation can be closed when we receive ATF's procedures for notifying IAD, MMB, ATF JSOC, DOJCERT, and NCIC, if appropriate, when accountable property is lost, stolen, or identified as missing during periodic inventories. The procedures should specify the requirement for

the reporting and how proper reporting will be verified. The procedures should also include accountable property identified as missing during periodic inventories.

2. **Resolved.** We recommended that ATF ensure that for each loss, Materiel Management provides Internal Affairs with the Report of Survey Information needed to conduct an investigation. This recommendation is resolved based on ATF's agreement with it.

Similar to Recommendation 1, it is not clear to us how the planned corrective action will both require and verify that Reports of Survey and other necessary information are provided to Internal Affairs. It is also not clear whether the planned corrective action will include accountable property identified as missing during periodic inventories, as we believe is appropriate.

This recommendation can be closed when we receive ATF's procedures for ensuring that the Materiel Management Branch provides Internal Affairs with the Report of Survey and other needed information for each loss. The procedures should specify the requirements for providing documentation to Internal Affairs and verifying the documents were provided. The procedures should also include accountable property identified as missing during periodic inventories.

3. **Resolved.** We recommended that ATF implement a written policy for reporting losses of ammunition to Internal Affairs for investigation. This recommendation is resolved based on ATF's agreement with it.

ATF stated that it is revising reporting procedures and requiring new inventories to establish a baseline for perpetual inventories. However, it is not clear to us whether the corrective action plan will include procedures for reporting ammunition identified as missing during an inventory, which we believe should be included.

We have separately received revised procedures requiring the reporting of ammunition losses resulting from break-ins or thefts. This recommendation can be closed when we receive ATF's revised procedures for reporting losses of ammunition to Internal Affairs that include ammunition identified as missing during an inventory.

4. **Resolved.** We recommended that ATF implement procedures to determine the contents of lost, stolen, and missing laptop computers. This recommendation is resolved based on ATF's agreement with it.



ATF stated that its current procedures require employees to provide reports summarizing the loss of an ATF laptop computer, the type of information it contained, whether the information was sensitive or personally identifiable information, and whether the laptop computer was encrypted. ATF stated that those reports are submitted to the Help Desk and subsequently reported to DOJCERT. This procedure is available to all ATF employees through the ATF Intra-web and is referenced in a March 2007 letter that we reviewed during our audit from the ATF Chief Information Officer (CIO). However, it is not clear to us who at ATF will determine the contents of the laptop computers and how the contents will be documented.

This recommendation can be closed when we receive ATF's procedures for determining and documenting the contents of lost, stolen, or missing laptop computers. These procedures should contain sufficient detail to identify and protect any information on lost or stolen laptop computers. In addition, the procedures should specify who is responsible for completing the required actions and who will determine and document the contents of the computers. We also request a copy of the procedure as posted on the ATF Intra-web.

5. **Resolved.** We recommended that ATF require that lost, stolen, or missing weapons and laptop computers are appropriately entered into NCIC. This recommendation is resolved based on ATF's partial agreement with it.

ATF implied that our results included some items not reported to NCIC because those items were recovered shortly after being reported lost or stolen. This is incorrect. We clearly reported that seven weapons did not require an NCIC entry because ATF recovered those weapons shortly after the reported loss. We also identified five weapons not reported to NCIC and never subsequently recovered or recovered after a period of years.

ATF's response stated that ATF plans to revise its reporting procedures and will rely on its JSOC to ensure that all lost or stolen weapons and laptop computers are recorded timely in NCIC. Although ATF plans to revise its reporting procedures to include all lost and stolen weapons and laptop computers, it is not clear to us that the procedures will also apply to weapons and laptop computers identified as missing during an inventory, as we believe is appropriate. This recommendation can be closed when we receive ATF's revised procedures requiring that all lost, stolen, or missing weapons and laptop computers be reported to NCIC,

including weapons and laptop computers that are identified as missing during an inventory.

6. **Resolved.** We recommended that ATF develop procedures for updating the property management system to ensure accurate and complete weapon and laptop computer records are maintained. Although ATF stated that it disagreed with the recommendation, it also identified plans for corrective action intended to ensure the accuracy of property management data. Despite its stated disagreement, this recommendation is resolved based on ATF's planned corrective action as discussed below.

ATF noted that it disagrees with the recommendation because current procedures are sufficient to address the recommended corrective action. However, ATF also identified additional plans to remind all employees to enter, update, and maintain accurate data; develop and implement standardized on-line training for property custodians; and revise procedures to require that property custodians be designated, at a minimum, at the level of branch or field office. In its response, ATF notes that "A fuller contingent of property custodians will enhance ATF's ability to manage property and ensure accurate and complete computer records." Given that all these actions, and particularly the one pertaining to property custodians, appear sufficient to address the clear intent of our recommendation, we believe the appropriate status for this recommendation is "resolved" based on the corrective action proposed by ATF.

This recommendation can be closed when we receive documentation that: (1) employees have been reminded to enter, update, and maintain accurate property data; (2) standardized training has been developed and implemented for property custodians; and (3) procedures have been revised to require that property custodians be designated, at a minimum, at the branch or field office level. ATF's next update on these recommendations should provide information about when each of the three actions is expected to be completed.

7. **Resolved.** We recommended that ATF locate or report as missing the sampled items not found during the audit. This recommendation is resolved based on ATF's partial agreement with it.

We agree with ATF's corrective action plan to improve the accountability of assets by appointing additional staff and establishing procedures to oversee the contractor that provides laptop computers to ATF staff.

However, we disagree with ATF's characterization of the 4 weapons and 23 laptop computers not located or verified during our audit.

ATF stated that "Those items not physically inspected were characterized as lost by the audit team. Subsequently to that, ATF employees participated in an exhaustive effort with the audit team in faxing laptop verification certificates to the Atlanta Regional Audit Office." In fact, during our on-site work at ATF offices we did not characterize as "lost" those items that were not available for physical inspection, and we do not characterize those items as "lost" in the audit report. For items that were not available for us to inspect personally during site visits, we requested signed confirmation memoranda for the weapons and laptop computers in our sample. Each confirmation memorandum was to include identifying information about each item and was to be signed by two people attesting to the identifying information. We did not accept as verified any property that we could not physically inspect and for which ATF could not produce a complete and properly signed confirmation memorandum.

This recommendation can be closed when ATF provides documentation that each of the 27 items has been either located or reported as lost, stolen, or missing. Documentation should consist of an acceptable confirmation memorandum, signed by two people attesting to the identifying information on each item; documentation that the item has been reported as lost, stolen, or missing; or other documentation showing the item is accounted for.

8. **Resolved.** We recommended that ATF ensure that all laptop computers are encrypted. This recommendation is resolved based on ATF's agreement and its plan to complete encryption for networked laptop computers. However, ATF did not address laptop computers that are not networked. In its next update on these recommendations, ATF should provide further information about how and when the non-networked laptop computers will be encrypted, or provide the justification for not encrypting some of those laptop computers. The recommendation can be closed when we receive documentation that all of ATF's laptop computers have been encrypted or justified as exempt from encryption.
9. **Resolved.** We recommended that ATF ensure complete, accurate, and timely reports are submitted to the DOJ CIO containing all appropriate ATF laptop computers authorized to process classified information. This recommendation is resolved based on ATF's agreement and its plan to

review its procedures to determine how the prior omission occurred and make the necessary adjustments to prevent future occurrences. This recommendation can be closed when we receive the results of ATF's review regarding how the omission occurred and a copy of the adjustments to the procedures ATF determines are appropriate to prevent future occurrences. If this is not completed prior to ATF's next update on these recommendations, we request a planned completion date for this action.

10. **Resolved.** We recommended that ATF ensure that complete, accurate, and timely semiannual reports identifying lost, stolen, or missing weapons and laptop computers are submitted to the DOJ Security Office and Justice Management Division. This recommendation is resolved based on ATF's agreement and its plan to prepare semiannual reports based on recent modifications to its property management system. The recommendation can be closed when we receive a copy of the report due to the Department in September 2008.
11. **Resolved.** We recommended that ATF develop procedures to ensure it completes accurate and timely incident reports summarizing the loss of ATF laptop computers and submits those reports to DOJCERT, as required by DOJ policy. This recommendation is resolved based on ATF's agreement and its plan to revise its reporting process, which is specified in the response to recommendations 1 and 2. This recommendation can be closed when we receive the revised procedures outlined for recommendations 1 and 2.
12. **Resolved.** We recommended that ATF maintain documentation for all disposed property, document data clearing of disposed laptop computers, and update active and disposed property records, as necessary. This recommendation is resolved based on ATF's partial agreement.

We are concerned that ATF's response indicates only that it retains records in accordance with various standards and implies that we are requesting corrective action for records handled in accordance with those standards. ATF should note that we specifically excluded from our audit findings any records of property disposition that were outside ATF's record retention period. Our audit found that there were no disposition records for 5 weapons and 21 laptop computers that were disposed of during the then-current and two prior fiscal years (2005, 2006, and 2007). In its next response to these recommendations, we

request that ATF provide a plan to prevent these deficiencies in current records.

Also, ATF's response does not address the portion of the recommendation pertaining to documenting data clearing of disposed laptop computers. Our audit tested 116 of the 149 laptop computer disposals documented during the then-current and two prior fiscal years (2005, 2006, and 2007). Of the 116 laptops we tested, ATF provided certificates of data clearing for only 4 (3 percent). In its next response to these recommendations, we request that ATF provide a plan to document that data has been cleared from laptop computers prior to disposition.

Finally, in its response to this recommendation ATF did not address the issue of updating active and disposed property records. However, we believe this action is adequately addressed in ATF's response to recommendation 6.

This recommendation can be closed when recommendation 6 is closed and when ATF provides evidence for how it will maintain documentation for all disposed property and document data clearing of disposed laptop computers.

13. **Resolved.** We recommended that ATF develop procedures and maintain documentation to ensure that separated employees return all weapons, laptop computers, and other accountable property before they separate from ATF. This recommendation is resolved based on ATF's agreement with it.

We are concerned that ATF's response focuses on reviewing the internal control process to ensure that returns of property are documented by supervisors and entered into the property management system. We found during our audit that it was not possible to identify property items in the system by employee name after the person had separated. Therefore, revisions to the process should include an alternate record of the serial and property identification numbers of accountable items returned by separating employees.

This recommendation can be closed when we receive the results of the review of internal controls and revised procedures that will ensure ATF can identify the specific items returned by each separated employee.

14. **Resolved.** We recommended that ATF enforce current requirements to perform annual inventories of ammunition and maintain a perpetual inventory system at all ammunition storage locations to ensure accurate and complete records. The recommendation is resolved based on ATF's agreement with it.

ATF's response indicates that it will conduct an inventory by October 15, 2008, and that the ATF Office of Inspection will add the inspection of ammunition control logs to its office review process. We understand that inspections occur every 3 years for each office. We are concerned that the response does not specify how ATF will enforce its policy that annual ammunition inventories be performed, and does not specify how it will ensure that a perpetual inventory is maintained.

This recommendation can be closed when we receive documentation demonstrating how ATF will ensure annual inventories of ammunition are performed and perpetual inventory records are maintained.