



**THE DRUG ENFORCEMENT ADMINISTRATION'S  
CONTROL OVER WEAPONS  
AND LAPTOP COMPUTERS  
FOLLOW-UP AUDIT**

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

Audit Report 08-21  
March 2008



# THE DRUG ENFORCEMENT ADMINISTRATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS FOLLOW-UP AUDIT

## EXECUTIVE SUMMARY

In 2001, at the request of the Attorney General, the Office of the Inspector General (OIG) conducted audits of the controls over weapons and laptop computers at the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Federal Bureau of Prisons, and the United States Marshals Service. These audits resulted from concerns about the Department of Justice's (DOJ) accountability for weapons and laptop computers. The OIG issued separate reports concerning each component and an overall report summarizing the results.

In August 2002 we issued the report concerning the DEA's control over weapons and laptop computers. Our report identified weaknesses in the DEA's management of weapons and laptop computers, including purchases, receipts and assignments, transfers, returns of property from employees leaving the DEA, physical inventories, and property disposals.<sup>1</sup> We made 22 recommendations in our 2002 report to help the DEA address these deficiencies, such as reiterating policy regarding procedures and controls over weapons and laptops, ensuring losses were reported as required, and maintaining complete, accurate, and current inventory records.

### Results in Brief

The purpose of this follow-up audit was to determine whether the DEA has made progress since our 2002 audit concerning its control over weapons and laptops. To assess the DEA's progress, we performed a comparative analysis using the findings from our 2002 audit and this follow-up review. We found that the DEA's rate of loss for weapons more than doubled since the 2002 audit, while the rate of loss for laptop computers declined by more than 50 percent.

Our 2002 audit found that DEA employees were not reporting lost or stolen weapons to the DEA in a complete and timely manner. In addition, the DEA had failed to ensure that all lost or stolen weapons were entered in

---

<sup>1</sup> U.S. Department of Justice Office of the Inspector General. *The Drug Enforcement Administration's Control over Weapons and Laptop Computers*, Audit Report 02-28, (August 2002).

the National Crime Information Center (NCIC) database. During our follow-up audit, we found that these same weaknesses have persisted. The DEA has not adequately and promptly reported incidents of lost or stolen weapons and laptop computers to DEA headquarters and has not ensured that lost or stolen property was entered in the NCIC database. The DEA's failure to report losses and enter relevant information in the NCIC database also reduces the DEA's chances of recovering this lost property.

The DEA Board of Professional Conduct's case files did not contain information for 226 of the 231 lost or stolen laptop computers regarding either the content or whether or not the laptop was encrypted. Therefore, the DEA could not provide assurance that 226 of the laptops identified as lost or stolen during our review period did not contain sensitive or personally identifiable information (PII). In addition, since the DEA did not begin to install encryption software on its laptops until November 2006, few of the laptops lost or stolen during our review period were protected by encryption software.

In our 2002 audit we reported that the DEA had significant weaknesses in its internal controls over weapons and laptops. This follow-up audit found that while the DEA has improved its controls and procedural compliance in its physical inventories, the DEA has failed to retain adequate documentation necessary to support laptop acquisitions, disposals, and losses. We also found that because the DEA failed to document laptop serial and property numbers on the DEA Employee Clearance Record forms, the DEA was not ensuring that assigned laptops were returned.

In this follow-up report, we made seven recommendations designed to reinforce the need for the DEA to improve its internal controls governing the accountability of weapons and laptop computers. We again emphasized the need to submit timely and accurate DEA Forms 29 and ensure all losses are promptly entered into the NCIC database. In addition, DEA must submit complete and accurate semiannual Department Theft and DOJ Computer Emergency Response Team (DOJCERT) incident reports.

Our report contains detailed information on the full results of our review of the DEA's control over weapons and laptop computers. The remaining sections of this Executive Summary address our audit approach and summarize our audit findings.

## Audit Approach

In this follow-up audit we conducted our fieldwork at DEA headquarters, headquarters-level offices, and six field division offices. The scope of this 2007 follow-up audit covered the 66-month period between January 2002 and June 2007.

Our work included determining the DEA's practices and procedures for responding to losses and assessing the DEA's internal controls over its weapons and laptops. We conducted physical inventories and tested the accuracy and completeness of DEA records for weapons and laptops. We tested DEA-owned and assigned weapons, as well as personally owned weapons authorized for official purposes. We also queried the NCIC database to determine if lost, stolen, or missing weapons and laptops were entered into the database in a timely manner.

Further, we assessed the DEA's internal and external reporting practices for lost or stolen weapons and laptops. Specifically, we evaluated whether the DEA promptly and appropriately notified the DOJ of incidents of loss. Our audit also examined the actions taken by the DEA in response to lost or stolen weapons and laptops, including whether the DEA determined what information was on the laptop and whether any discipline was imposed. Additionally, we reviewed the DEA's practices for ensuring that DEA-owned weapons and laptops were returned to the agency by employees leaving the DEA.

Where appropriate, we also compared results from this follow-up review of the DEA to results in our February 2007 follow-up audit of the FBI's controls over its weapons and laptop computers.<sup>2</sup> Specifically, we computed and compared the rates of losses for weapons and laptops per 1,000 agents per year for these two agencies, and we evaluated the circumstances regarding reported losses.

Appendix I contains more information on our audit objectives, scope, and methodology.

---

<sup>2</sup> 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).

## **Property Management Regulations and Responsibility**

The Office of Management and Budget Circular A-123 and the DOJ's Justice Property Management Regulations require DOJ components to issue detailed operating procedures for protecting federal property against fraud, waste, and abuse. The DEA Property Management Handbook contains guidelines for the general management of property, stating that weapons and laptop computers must receive an asset number, be entered into one of the DEA's independently operated property subsystems, and be inventoried annually.<sup>3</sup>

The Firearms Training Unit is responsible for the overall management of the DEA's inventory of weapons and the DEA's weapon property system – the Weapons Database, which includes information such as the weapon make, model, serial number, name of the responsible custodian, location, acquisition date, and cost. Each of the DEA's field divisions has a designated Primary Firearms Instructor assigned to control the weapons inventory for that division. For each headquarters unit, division office, district office, resident office, and foreign country office, a Property Custodial Assistant is designated for property management, including laptop computers. Information on laptop computers is maintained in the DEA's Fixed Asset Subsystem, including the laptop asset number, serial number, manufacturer, model number, acquisition date, cost, physical location, property condition, and the name of the responsible Property Custodial Assistant.

### **DEA Lost or Stolen Weapons and Laptop Computers**

Our 2002 audit found that over a 26-month period the DEA had 16 weapons and 229 laptop computers lost or stolen. In this follow-up audit, we determined that over a 66-month period 91 weapons and 231 laptop computers were lost or stolen. Comparing the results of these two audits, we found that the DEA's monthly rate of loss for laptop computers decreased by more than 50 percent, while the rate of loss for weapons more than doubled from 0.61 to 1.37 weapons a month as shown in the following table.<sup>4</sup>

---

<sup>3</sup> At the time of our audit, the DEA Property Management Handbook was being revised.

<sup>4</sup> Because the audit periods were different lengths, we analyzed the rate of loss on an equivalent monthly basis. Our review period for the 2002 audit covered 26 months, from October 1, 1999, to November 30, 2001. Our review period for the follow-up audit covered 66 months, from January 1, 2002, to June 30, 2007.

**DEA MISSING WEAPONS AND LAPTOP COMPUTERS  
2002 AUDIT COMPARED TO FOLLOW-UP AUDIT**

Category	Number of Lost or Stolen Items Reported		Losses Reported Per Month	
	2002 Audit	Follow-up Audit	2002 Audit	Follow-up Audit
Lost Weapons	4	22	0.15	0.33
Stolen Weapons	12	69	0.46	1.04
<b>Total Lost or Stolen Weapons</b>	<b>16</b>	<b>91</b>	<b>0.61</b>	<b>1.37</b>
Lost Laptop Computers	229 <sup>5</sup>	206	8.81	3.12
Stolen Laptop Computers	0	25	0	0.38
<b>Total Lost or Stolen Laptops</b>	<b>229</b>	<b>231</b>	<b>8.81</b>	<b>3.50</b>

Source: OIG analysis of DEA Board of Professional Conduct case files

*Weapons Losses*

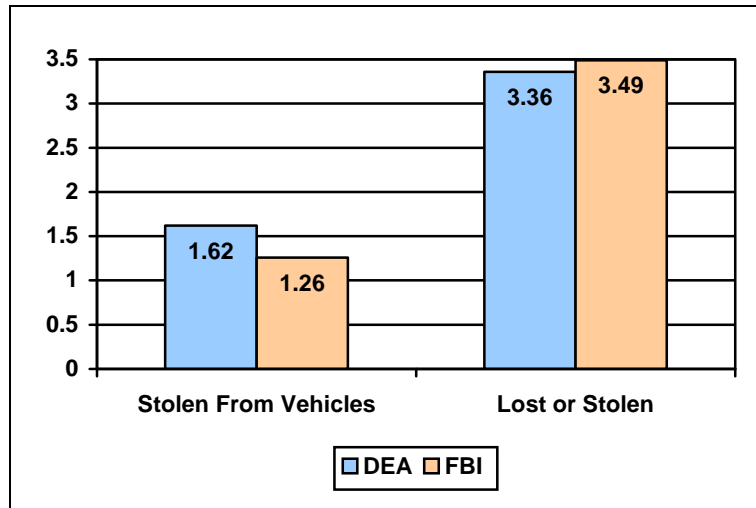
Our follow-up review examined the DEA Board of Professional Conduct case files regarding lost or stolen weapons and laptops. We found many instances when losses occurred despite reasonable precautions taken by DEA employees.<sup>6</sup> However, we also found instances when losses resulted from employees failing to follow DEA policy. For instance, the DEA Agents Manual, Section 6122.42 Firearms Security, Safety and Storage, specifically states that DEA-issued and authorized personally owned pistols may not be left unattended or temporarily stored in an official government or privately owned vehicle. Our review found that 44 of the 69 stolen DEA weapons were taken from vehicles. This was similar to our 2007 follow-up audit of the FBI, which reported 58 weapons stolen from vehicles. We determined that the DEA had 1.62 weapons stolen from vehicles per 1,000 agents per year, while the FBI had a lower rate of 1.26 weapons stolen from vehicles per 1,000 agents per year. However, in total the FBI had 3.49 lost or stolen weapons per 1,000 agents per year, while the DEA had 3.36 weapons.

---

<sup>5</sup> The DEA reported that 229 laptops were unaccounted for during the prior audit. The DEA was unable to provide any details as to the number of lost versus stolen laptops.

<sup>6</sup> Board case files contain copies of the DEA Form 29, a property/accident synopsis form that briefly describes the incident, what was lost or stolen, the responsible individual, the proposed disciplinary action, and the final disciplinary action taken. This file also includes a copy of the letter of proposed disciplinary action, documents regarding the proposed disciplinary action, and copies of any other investigation results.

**WEAPONS STOLEN FROM VEHICLES AND TOTAL LOST OR STOLEN  
PER 1,000 AGENTS PER YEAR**



Source: OIG analysis of DEA and FBI follow-up audit data

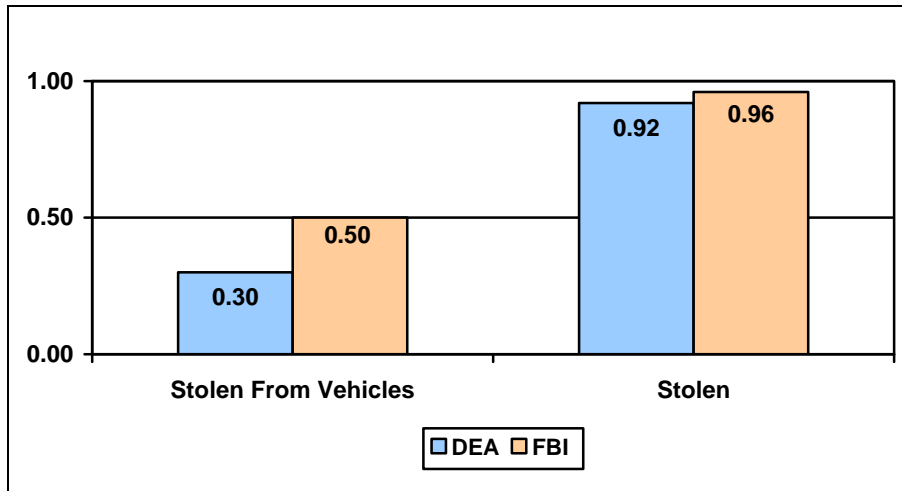
*Laptop Computer Losses*

Similar to the lost and stolen weapons, we found that many laptop computer losses were avoidable if DEA employees had exercised appropriate diligence and complied with DEA policy. For example, one laptop was left in a taxi and another was stolen from checked luggage. However, we were unable to analyze the circumstances behind the vast majority of laptop losses because the DEA could not provide us with information for 206 of 231 missing laptop computers (89 percent). The DEA identified 149 of these 206 laptops as missing when conducting annual laptop inventories. The remaining 25 laptop computers (11 percent) were reported as stolen from vehicles and other locations such as hotels. Appendix IV includes more detail on reported laptop losses.

Comparing the DEA and FBI follow-up audit results for stolen laptop computers, we found that the DEA and FBI both averaged nearly 1 laptop computer stolen per 1,000 agents annually. In total, the DEA reported 8 laptops stolen from vehicles while the FBI reported 23 laptops.



**LAPTOP COMPUTERS STOLEN FROM VEHICLES AND TOTAL STOLEN  
PER 1,000 AGENTS PER YEAR**



Source: OIG analysis of DEA and FBI follow-up audit data

### **Reporting Lost or Stolen Weapons and Laptops**

DEA policy requires the responsible employee to file a police report in the jurisdiction where the loss or theft of a weapon or laptop occurred. The employee or their immediate supervisor also must ensure the weapon is entered in the NCIC database by the local police agency responsible for the jurisdiction in which the loss or theft was reported.<sup>7</sup> Within 48 hours of the event, the responsible employee also must submit Part 1 of the DEA Form 29, which is used to record pertinent information related to the loss. (Appendix XI contains a copy of DEA Form 29.)

In October 2002 the DEA Administrator issued a memorandum requiring laptop losses to be reported to the DEA Board of Professional Conduct and the DEA Office of Professional Responsibility within 48 hours of an incident. In the past, lost or stolen weapons and laptops reported by the DEA field offices were only referred by the Board of Professional Conduct to the DEA Office of Professional Responsibility if documentation suggested any form of misconduct related to the loss, theft, or destruction of a weapon or laptop.

---

<sup>7</sup> The 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, which are then accessible to law enforcement agencies nationwide.

On March 30, 2007, the DEA issued an additional policy clarifying reporting responsibilities for lost or stolen weapons. This policy requires all lost or stolen weapons to be referred to the DEA Office of Professional Responsibility, which determines whether it will conduct an investigation or assign the reporting office to perform the investigation.

Data regarding lost or stolen weapons and laptops also must be promptly entered into NCIC so that information is available to law enforcement personnel. The DEA is a non-record entering agency for NCIC, meaning that DEA employees do not enter data into the system, but rather must rely on local law enforcement agencies to perform the task.

### *Weapon and Laptop Losses Not Reported in a Timely Manner*

Similar to our finding in the first DEA audit, we found during this follow-up audit that the DEA failed to ensure that lost or stolen weapons were reported in a complete and timely manner. While a DEA Form 29 was completed for each of the 91 missing weapons, 37 of the 81 forms (46 percent) were not completed within the 48-hour timeframe.<sup>8</sup> We determined that 2 weeks elapsed between the time of the incident and when DEA personnel reported the loss in 19 of the 37 forms (51 percent) submitted after the 48-hour deadline. This failure can hinder timely investigations regarding each loss. In addition, 13 of the 81 forms (16 percent) did not contain critical information such as the correct serial number or whether the weapon was entered into NCIC.

We found similar issues with respect to missing or stolen laptops during our follow-up audit. For example, of the 110 DEA Forms 29 examined for the 231 laptop computers reported missing, 9 forms were submitted within the required timeframe and 31 forms were submitted late.<sup>9</sup> Of those 31, 20 were filed anywhere from 15 days to 4.7 years late. However, due to incomplete information, we were unable to determine if the remaining 70 forms were submitted within the 48-hour timeframe.

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

Since October 2002, the DEA has required a statement identifying whether a lost or stolen laptop contained DEA sensitive or classified

---

<sup>8</sup> We reviewed 81 DEA Forms 29 reporting the loss of 91 weapons. Multiple weapons lost in a single incident are reported on a single DEA Form 29.

<sup>9</sup> Several cases reported multiple laptops on one DEA Form 29.

information when reporting the incident. However, we found that DEA Board of Professional Conduct files contained these statements for only 5 of the 231 laptop computers reported lost or stolen during this 66-month review period. Of the five statements submitted, DEA records indicated that four laptops did not contain sensitive or classified information while the fifth contained sensitive case information.

We asked DEA senior managers what the DEA did to determine the contents of the remaining 226 lost or stolen laptop computers. The DEA was unable to provide information regarding what was on the laptops. The DEA told the OIG that “DEA is unable to provide, with certainty, assurance that the content of many of these laptops is not sensitive information because it does not remotely (in an automated manner) manage its laptops.” The DEA’s Security Programs Information Security Section Chief stated that an investigator generally attempts to determine what information may have been lost or compromised. However, the Section Chief told us there is no way to determine exactly what was on the laptop unless it is recovered.<sup>10</sup> We believe the DEA’s inability to determine what was on the many stolen or missing laptops was a significant failure.

### *Encryption of Laptop Computers*

According to a DEA policy implemented on July 30, 2007, all DEA laptop computers used to process sensitive information must be encrypted.<sup>11</sup> As shown in the following table, we determined that as of December 2007, 3,393 of the DEA’s 5,287 laptop computers had been encrypted. As of December 2007, the DEA also reported that 155 additional laptops were in the process of being encrypted, while the remaining 1,739 laptops were exempt from the encryption requirement because they were not used to process sensitive information. According to DEA policy implemented on July 30, 2007, these laptops are used by Special Agents or Investigative Technology Specialists exclusively to support electronic surveillance and other digital monitoring functions.

---

<sup>10</sup> In addition, as we explain in the next section, nearly all of the 231 laptop losses reported during our 66-month review period occurred before DEA began encrypting laptops.

<sup>11</sup> On March 28, 2007, the DEA submitted a memorandum to the DOJ Chief Information Officer requesting a 60-day extension to May 31, 2007, for meeting the DOJ requirement to ensure that all unclassified laptops had encryption to protect sensitive data. This memorandum noted that the DEA began encrypting laptop computers in mid-November 2006. The DOJ Chief Information Officer approved the DEA’s request. According to DEA policy implemented on July 30, 2007, all laptop computers used to process sensitive information must be encrypted.

**DEA LAPTOP COMPUTERS ENCRYPTED**  
**Laptops in Use as of December 2007**

Category	Number	Percent
Encrypted	3,393	64%
Exempt	1,739	33%
In Progress <sup>12</sup>	155	3%
<b>Total</b>	<b>5,287</b>	<b>100%</b>

Source: OIG analysis of DEA Security Information Office data

During our fieldwork in this follow-up audit, we attempted to assess whether laptops reported lost or stolen were encrypted to protect the data and, if not encrypted, what data was on the laptops. Our assessment of the contents of laptops at the field sites we visited consisted of a visual inspection of programs and recently modified files. Our review did not examine the entire contents of the laptops.

We found that 79 of 164 laptops we sampled were not encrypted. Of the 79 laptops that were not encrypted, we identified at least 5 that contained sensitive case-related information or PII. Our limited testing did not find sensitive case information or PII on the remaining 71 laptops.

*Entering Losses into NCIC*

During the initial audit in 2002, we determined that 6 of the 16 lost or stolen weapons were not entered into the NCIC database. In this follow-up audit we queried the NCIC database for the 91 lost or stolen weapons and found that 11 were not entered into the database, while 7 of the weapons were entered in the database with incorrect serial numbers.

Regarding laptops, we found that only two DEA Forms 29 contained sufficient documentation showing that the laptops were entered into NCIC. We queried the NCIC database for the lost or stolen laptops and found that 229 of the 231 laptops reported lost or stolen did not have a record in the NCIC database as required by DEA policy.

**Internal Controls**

Internal controls for management of accountable property are intended to provide reasonable assurance that resources are adequately

---

<sup>12</sup> DEA officials informed us that these laptops were assigned to personnel in temporary duty status, have compatibility issues with the encryption software, require additional memory, or need batteries.

safeguarded and that reliable data on this property is maintained and properly reported. During this audit, we assessed the DEA's internal control structure and compliance with procedures for conducting inventories, maintaining sufficient and accurate property records, reporting incidents of loss to the DOJ, accounting for the disposal of property, and ensuring exiting employees remit DEA-issued property.

In our 2002 audit report we found that the DEA did not physically inventory weapons on an annual basis and that the DEA's separation of duties over weapons inventorying at the Firearm Training Unit was inadequate. We also found that although weapons were excessed to other law enforcement agencies with proper documentation, the DEA failed to ensure that the other agencies actually received the weapons. In addition, although there was a category for weapons on the DEA Employee Clearance Record, (DEA Form 171a, see Appendix XII), the form did not require details of the weapons returned or provide details of the accountable property retrieved from an employee leaving the DEA.<sup>13</sup> We examined each of these issues again in the current audit.

### *Physical Inventories*

DEA regulations require an annual inventory of all sensitive capitalized assets and sensitive property items, which include weapons and laptop computers. In our follow-up audit, we reviewed DEA-wide inventory reports from 2002 through 2006 and determined that physical inventories of weapons and laptops were conducted as required.

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

In our 2002 audit report, we determined that the DEA's financial system was not integrated with its weapons inventory system – the Weapons Database – to ensure inventory accuracy. In addition, the financial system did not include an audit function that allowed edits made to the Weapons Database to be tracked by an automated exception report. The DEA's financial system also had not been fully integrated with its Fixed Asset Subsystem. As a result, the systems did not automatically verify that the number of laptops actually purchased agreed with the number of items placed into inventory. To improve the controls over its weapons and laptop computer inventories, we recommended that the DEA develop internal

---

<sup>13</sup> The DEA Employee Clearance Record is a form used by DEA to document that an exiting employee has returned badges, credentials, weapons and other property and has cleared various internal departments such as finance and procurement.

controls to ensure the reliability of inventories in the Weapons Database and integrate its financial and property management systems so that inventory would be routinely updated as laptops were purchased.

In our follow-up review, we found that the DEA's financial system still is not integrated with its Weapons Database. However, we consider control procedures, such as providing field components with inventories for reconciliation purposes and verifying the accuracy of the Weapons Database by Primary Firearm Instructors through a physical inventory implemented by the DEA since our prior audit, to be sufficient for ensuring that information in the Weapons Database is accurate and complete. In addition, all entries into the Weapons Database were completed by the Firearms Training Unit at Quantico, Virginia, which incorporated appropriate separation of duties.

With respect to laptops, we found that the DEA's financial system is fully integrated with its Fixed Asset Subsystem, which accounts for laptops, and the DEA had properly segregated the duties of staff taking physical inventories, performing reconciliations, and modifying the property management system.

#### *Accuracy and Completeness of Inventory Records*

In our 2002 audit we tested the accuracy and completeness of the Weapons Database and the Fixed Asset Subsystem. On a sample basis we selected weapons from the Weapons Database and laptop computers from the Fixed Asset Subsystem to physically verify their existence. The DEA provided all weapons and laptop computers for our physical verification.

During our follow-up audit we tested 4,331 DEA-owned and 763 personally owned weapons. We were able to verify 4,320 (99.7 percent) of the sampled DEA-owned weapons and all 763 of the personally owned weapons we sampled. The DEA was unable to account for 11 weapons in our sample. The DEA believed seven of these weapons were destroyed but had no supporting documentation concerning their destruction. For the remaining four weapons, two were issued to Special Agents on assignment, one weapon was an erroneous entry into the Weapons Database, and the last weapon was a non-functional training weapon that could not be located.

We conducted similar testing on a sample of DEA laptop computers. Our sample comprised 3,007 of the DEA's 7,381 total laptop computers. We considered that the DEA accounted for the laptop if it was able to present the laptop for our verification or provide documentation supporting that the laptop existed. We also accepted documentation showing that the laptop

was lost, stolen, destroyed, or surplused after the date of our statistical sample. The DEA was unable to account for 42 of the 3,007 sampled laptops (1 percent). Additionally, we found 20 laptops assigned to DEA headquarters components were not entered in the Fixed Asset Subsystem, and the DEA took immediate corrective action by adding these laptops to the inventory.

### *Reporting Losses to DOJ*

DOJ regulations require all components to submit to DOJ semiannual reports on January 1 and July 1 summarizing the loss or theft of government property that occurred within the preceding 6 months.<sup>14</sup> In our 2002 audit, we found that the DEA did not submit any semiannual Department Theft Reports for 1999 and 2000, and the first semiannual report for 2001 was submitted 36 days late. In addition, the semiannual reports submitted by the DEA were inaccurate with respect to the number of weapon losses.

For this follow-up audit we again tested the DEA's submission of semiannual Department Theft Reports. We also analyzed the DEA's compliance with DOJ regulations requiring all components to immediately notify the Department of Justice Computer Emergency Response Team (DOJCERT) of incidents involving the loss of laptops.

DOJ Semiannual Reports – Our follow-up review found that the DEA has not corrected its deficiency in reporting to the DOJ on the weapons and laptop computers that were lost or stolen during semiannual reporting periods. During the time period covered by our audit, 11 semiannual Department Theft Reports were required to be submitted to the DOJ. However, the DEA was only able to provide, and DOJ only had on file, 3 of the 11 semiannual reports required during our testing period.

We reviewed the three semiannual Department Theft Reports submitted by the DEA during our audit period, and found that one report was complete, but the other two reports contained errors and omissions. While two of the three reports were submitted in a timely manner, we were unable to determine if the third report was submitted when required. We asked the DEA Deputy Assistant Administrator, Office of Administration, about the remaining eight reports. She told us that the administrative clerk

---

<sup>14</sup> DOJ Order 2630.2A, Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures.

who prepared the semiannual theft reports typed over the prior report and failed to retain a paper or electronic copy of the reports.

In addition, we found that the DOJ Justice Management Division was not aware of 67 weapons and 176 laptops that were lost or stolen during our review period because the DEA did not submit the required semiannual Department Theft Reports. Only 20 weapons and 24 laptops were reported to the Justice Management Division as required by DOJ regulations.

DOJCERT Notification - The DOJCERT assists in handling computer security incidents throughout DOJ. DOJCERT officials told us that DOJCERT was not required to track or report lost or stolen DEA laptops prior to May 2006. We identified 15 lost or stolen laptops from May 2006 through June 2007 that had been reported to the DEA's Board of Professional Conduct. However, DOJCERT only received reports from the DEA on three laptops during this time period.

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

In our 2002 audit report we found that DEA weapons excessed to other law enforcement agencies were supported by proper documentation. However, the DEA failed to follow up with these law enforcement agencies to ensure that the shipped weapons were actually received. We recommended the DEA ensure that the Firearms Training Unit document confirmations for receipt of the weapons. In our previous audit, we did not note any problems with the DEA's procedures for the disposal of laptops.

During our follow-up audit we selected a statistical sample of 295 weapons (43 destroyed and 252 surplus) from a universe of 7,300 excessed and destroyed weapons from January 2002 through February 2007. We found appropriate supporting documentation for all items tested, including confirmations from local law enforcement agencies that received the surplus weapons.

Additionally, we selected a sample of 166 laptops from a universe of 3,214 excessed and destroyed DEA laptop computers. The DEA could not provide sufficient supporting documentation for 15 of these 166 laptops tested (9 percent). For 13 of these 15 instances, we found that DEA did not retain any supporting documentation concerning the disposal. The DEA was unable to provide sufficient documentation to support the disposal for the other two instances.



We also found that the DEA's laptop disposal process is decentralized and that supporting documentation is maintained at each DEA location worldwide. During our testing, the DEA was unable to provide the OIG with requested disposal documentation in a reasonable amount of time. We believe the DEA should retain copies of all disposal documentation at centralized locations in each division office to manage the program more effectively, enable quicker reconciliations, and provide adequate audit trails. This added control would also elevate the DEA's oversight over laptop disposals and increase the overall accountability for excessing laptops.

### *Exit Procedures for Departing Employees*

In our 2002 audit report we found that although there was a category for weapons on the DEA's Employee Clearance Record, details of the weapon were not included on the form, such as serial numbers or property description. In addition, the form did not require information about what type of accountable property was retrieved from an employee who left the DEA.

During our follow-up audit we reviewed Employee Clearance Records at DEA field division offices for departing employees between January 1, 2005, and August 2, 2007. Our testing found that the DEA was appropriately completing the weapons section on the Employee Clearance Records, providing the DEA an important control over the weapons assigned to departing employees. However, we found that the DEA was still not documenting the Employee Clearance Records with specific details on laptop computers, such as serial number, property numbers, and make and model, returned by departing employees. Due to the lack of any specific details identifying laptop computers, we were unable to determine from this form whether DEA-issued laptop computers were returned by departing employees.

### **Conclusions and Recommendations**

Our follow-up audit found that the DEA decreased its rate of loss for laptop computers since our 2002 audit by more than 50 percent. In our prior audit report, we reported that the DEA could not determine if any of the lost, missing, or stolen DEA laptop computers resulted in a compromise of investigative information. In this audit, we found that the DEA still could not determine what was on its lost or stolen laptops. We found that for 226 of the 231 lost or stolen laptops reported in our follow-up audit review period, the DEA is unable to provide any assurance that the lost or stolen laptops did not contain sensitive information.

In addition, we found in this audit that the number of losses and the loss rate for weapons more than doubled from 0.61 to 1.37 per month since our last review.

The DEA has taken several steps since our 2002 audit to improve its ability to account for lost or stolen weapons and laptops computers. For instance, we found that the DEA performed annual physical inventories of weapons and laptops and reconciled these inventories to its financial system records.

However, this follow-up audit found that the DEA still requires significant improvements in its overall control over weapons and laptops. The DEA must ensure that DEA policy and guidelines are consistently enforced when an incident of loss or theft occurs. We found that the DEA did not sufficiently and promptly report incidents of loss to DEA headquarters or DOJCERT. Additionally, the DEA was not ensuring that lost or stolen weapons and laptops were entered in the NCIC database as required by DEA policy. These findings mirror weaknesses that we identified in our 2002 audit. Further, the DEA was unable to provide assurance that lost or stolen laptops did not contain sensitive information, failed to effectively maintain documentation for disposal of laptops, failed to submit required semiannual reports of weapon and laptop losses to the DOJ, and failed to adequately ensure that property was recovered from employees before separating from employment with the DEA.

This audit report contains seven recommendations related to ensuring compliance with DEA policies and reporting requirements. Specifically, we recommend that the DEA accurately and promptly report weapon and laptop losses to its headquarters and the appropriate DOJ components, revise its encryption policy to require that all laptops be encrypted, ensure that firearms and laptop property losses are entered in the NCIC database and verified by management for accuracy, and verify that property issued to departing employees is adequately documented and retrieved upon separation.

# TABLE OF CONTENTS

<b>INTRODUCTION</b> .....	<b>1</b>
Background.....	3
Property Management Regulations .....	4
Property Management Responsibility.....	4
Loss or Theft of Weapons or Laptop Computers .....	5
Automated Systems .....	6
OIG Audit Approach .....	7
<b>FINDINGS AND RECOMMENDATIONS</b> .....	<b>11</b>
<b>I.    DEA’s Response to Weapon and Laptop Losses</b> .....	<b>11</b>
DEA Lost or Stolen Weapons and Laptop Computers .....	11
Reporting Weapons and Laptop Computer Losses .....	13
Referring and Investigating Losses .....	20
Disciplining Employees Responsible for Losses .....	22
Conclusion.....	27
Recommendations .....	27
<b>II.   Internal Controls</b> .....	<b>29</b>
Physical Inventories .....	29
Reconciling Property Records to the Financial System .....	30
Accuracy and Completeness of Property Records in the Weapons Database and Fixed Asset Subsystem .....	32
Reporting Losses to DOJ .....	34
Disposals.....	37
Exit Procedures for Departing Employees .....	39
Conclusion.....	40
Recommendations .....	41
<b>STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS</b> .....	<b>42</b>
<b>APPENDICES</b> .....	<b>43</b>
Appendix I - Objectives, Scope, and Methodology .....	43
Appendix II - Abbreviations and Forms .....	47
Appendix III - Circumstances and Actions Taken for Lost and Stolen Weapons .....	49

Appendix IV	-	Circumstances and Actions Taken for Lost and Stolen Laptops.....	55
Appendix V	-	Analysis of Lost and Stolen DEA Weapons.....	71
Appendix VI	-	Analysis of Lost and Stolen DEA Laptops.....	75
Appendix VII	-	Lost and Stolen DEA Weapons Not Found in the NCIC Database.....	81
Appendix VIII	-	DEA-Owned Weapons and Laptop Computers Tested .....	83
Appendix IX	-	DEA Form 12, Receipt for Cash or Other Items .....	85
Appendix X	-	DEA Form 17, Firearms Control Record.....	87
Appendix XI	-	DEA Form 29, Personal Property Negligence/ Liability Assessment .....	89
Appendix XII	-	DEA Form 171a, Employee Clearance Record .....	91
Appendix XIII	-	DEA Form 609, Request for Authorization to Carry A Personally Owned Firearm .....	93
Appendix XIV	-	Drug Enforcement Administration Response .....	95
Appendix XV	-	Office of the Inspector General Analysis and Actions Necessary to Close the Report.....	101

# **DRUG ENFORCEMENT ADMINISTRATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS FOLLOW-UP AUDIT**

## **INTRODUCTION**

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

In August 2002 we issued our audit report on the DEA's control over weapons and laptop computers.<sup>15</sup> That report covered the 2-year period from October 1999 through November 2001. Our report disclosed losses of weapons and laptop computers and weaknesses in the DEA's management of this property, including purchases, receipts and assignments, transfers, returns of property from employees who leave the DEA, physical inventories, and disposals. We reported that the DEA:

- identified 16 weapons as lost, missing, or stolen during the 2-year period;
- identified that 229 laptop computers were unaccounted for;
- did not always report lost, missing, or stolen weapons to DEA management and DOJ officials in a complete and timely manner and did not ensure that all weapons reported as lost, missing, or

---

<sup>15</sup> U.S. Department of Justice Office of the Inspector General. *The Drug Enforcement Administration's Control over Weapons and Laptop Computers*, Audit Report 02-28, (August 2002).

stolen were entered in the National Crime Information Center (NCIC) database;<sup>16</sup>

- did not adequately segregate duties associated with maintaining its weapons inventory at its Firearms Training Unit in Quantico, Virginia;
- did not always conduct annual physical inventories of weapons or obtain written confirmation of receipt of weapons that were excessed to other law enforcement agencies; and
- did not maintain Employee Clearance Records with sufficient detail on remitted weapons and laptops for separated employees.

We made 22 recommendations to help the DEA address these deficiencies, including:

- reiterate to all DEA employees the guidelines for the security, safety, and storage of weapons and the requirements for reporting losses of DEA weapons as outlined in the DEA firearms policy;
- ensure the accurate and timely submittal of semiannual DOJ theft reports and the prompt entry of all lost, missing, or stolen weapons into the NCIC database;
- ensure that all purchases of laptops are entered into the Fixed Asset Subsystem inventory in a timely manner and that field division Property Custodial Assistants are advised in a timely manner by DEA headquarters of purchases and transfers of property items that pertain to their division; and
- ensure that details, such as property descriptions, DEA property numbers, and weapon serial numbers, are included on employee clearance records, and that confirmations from law enforcement entities affirming receipt of DEA excessed weapons are received and forwarded to the Firearms Training Unit.

---

<sup>16</sup> NCIC is a computerized index of criminal justice information, including criminal history information, fugitives, stolen property, and missing persons, that is available to federal, state, and local law enforcement and other criminal justice agencies.

Overall, the DEA stated that it agreed with our recommendations and would take corrective action to address the deficiencies. As of April 20, 2005, all 22 recommendations had been closed.

## **Background**

According to the DEA, its mission is to enforce the controlled substance laws and regulations of the United States and bring to the criminal and civil justice systems those organizations and principal members of organizations involved in the growth, manufacture, or distribution of controlled substances that are destined for illicit traffic in the United States. The DEA's Headquarters are in Arlington, Virginia. It has 227 domestic offices in 21 divisions throughout the United States and 86 foreign offices in 62 countries. As of June 23, 2007, the DEA had a total of 9,294 personnel (4,929 law enforcement) assigned to these offices.

In April 2007 the DEA had a total inventory of 14,449 weapons and 7,381 laptop computers. The inventory included semi-automatic handguns, shotguns, rifles, and training weapons that do not use live ammunition. Ninety-percent of DEA-owned weapons are issued to Special Agents, while 10-percent are unassigned and remain in the stock inventory at the Firearms Training Unit and at field locations.

Since 1973 DEA Special Agents also have been authorized to carry personally owned weapons for official use. The standards for personally owned weapons are the same as those for the DEA-owned weapons. DEA Special Agents are prohibited from carrying any personally owned weapon for official use other than those listed in the DEA Agent's Manual. In addition, DEA Special Agents must have an approved DEA Form 609 (Request for Authority to Carry a Personally Owned Firearm, see Appendix XIII) in their Primary Firearms Instructor file. Personally owned weapons were not included in our prior audit. In this follow-up audit, we included personally owned weapons because we noted that a significant number of Special Agents were authorized to carry personally owned weapons for official duty purposes.

Laptop computers are assigned to most Special Agents and other employees of the DEA. In April 2007 the DEA had an inventory of 7,381 laptop computers. An October 18, 2002, memorandum from the DEA Administrator stated that the storage of classified and other case sensitive information on laptop computers is strictly prohibited unless authorized by the DEA Office of Security Programs. Such an authorization must be laptop

specific to ensure that the laptop is certified and accredited to process sensitive or classified information.<sup>17</sup>

## **Property Management Regulations**

The Office of Management and Budget Circular A-123 requires agencies to develop and maintain effective internal controls to ensure that federal programs operate and federal resources are used efficiently and effectively to achieve desired objectives with minimal potential for waste, fraud, and mismanagement.<sup>18</sup> It also requires agencies to establish a management control system that ensures transactions are promptly recorded, properly classified, and accounted for in order to prepare accounts in a timely manner and reliable financial and other reports. The DOJ's Justice Property Management Regulations require DOJ components to issue detailed operating procedures for protecting federal property against fraud, waste, and abuse.

The DEA's Property Management Unit provides agency policy and guidance for laptop computers for DEA headquarters, domestic offices, and foreign offices. The DEA guidelines for the general management of property are contained in its Property Management Handbook, which was being revised and in draft status during our audit. The Accountable Personal Property and Equipment section of this handbook stated that weapons and laptop computers fall into the category of Accountable Personal Property and must receive an asset number and be entered into one of the DEA's independently operated property subsystems. The handbook also stated that both weapons and laptop computers must be inventoried annually.

## **Property Management Responsibility**

The draft version of the Property Management Handbook, which was still being reviewed and had not yet been issued as of January 29, 2008, defines property management as those functions of the government that deal with the acquisition, inventory control, protection, and disposition of government property. The Firearms Training Unit is responsible for the

---

<sup>17</sup> As of July 2007, the DEA stated that it had only five laptop computers that were specifically designated to process classified information. After 2007, sensitive data may be processed on encrypted laptop computers. Prior to this, approval had to be granted to process sensitive data on a DEA laptop. The DEA's Security Programs Information Security Section Chief told us that he was unaware of any approvals to process sensitive data.

<sup>18</sup> Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control.



overall management of the DEA's inventory of stock weapons and the DEA's weapon property system – the Weapons Database. Each of the DEA's 21 field divisions has a designated Primary Firearms Instructor assigned to control the weapons inventory for that division. For each headquarters unit, division office, district office, resident office, and foreign country office, a Property Custodial Assistant is designated for property management, including laptop computers.

### **Loss or Theft of Weapons and Laptop Computers**

When a weapon is lost or stolen, the responsible employee must immediately notify, through the chain of command, the employee's office head, who must ensure that the incident is immediately reported to the DEA headquarters Command Center. The Command Center is staffed 24 hours a day, 7 days a week and is responsible for immediately notifying the DEA's Board of Professional Conduct and Office of Professional Responsibility about the missing weapon. Within 48 hours of a loss, the responsible office head must notify the DEA's Board of Professional Conduct and the Office of Professional Responsibility and the discovering employee must provide details of the incident by completing Part 1 of the DEA Form 29, which is the DEA's standardized document for reporting lost and stolen property (see Appendix XI). In March 2007 the DEA issued interim policy designating the DEA Office of Professional Responsibility to manage the DEA's Lost or Stolen Firearm Program. The Office of Professional Responsibility determines whether it will conduct the investigation or require the responsible office to conduct the investigation.

Similar to a weapon loss, immediately upon discovery that a laptop computer has been lost or stolen, the responsible employee must immediately notify through the chain of command the office head, who must ensure the incident is reported to the DEA Help Desk. The Help Desk is then responsible for notifying the DEA Information Security Section. If the incident is reported outside normal business hours, the Help Desk should report the incident to the DEA Command Center instead of the Information Security Section. If the laptop computer contains PII or sensitive information, the Information Security Section or the DEA Command Center is required to report the incident within 1 hour to the DOJ Computer

Emergency Readiness Team (DOJCERT).<sup>19</sup> If the laptop computer contains classified information, the incident must also be reported to the Department of Justice Security and Emergency Planning Staff (SEPS). Within 48 hours, the responsible office head must notify the DEA's Board of Professional Conduct and the Office of Professional Responsibility, and the responsible employee must provide details of the incident in completing Part 1 of the DEA Form 29. The reporting office is responsible for conducting an investigation of the incident.

The DEA Board of Professional Conduct is responsible for reviewing the circumstances of the loss of firearms and laptops and making recommendations, such as assessing financial liability or recommending disciplinary action, to the DEA Office of Deciding Officials. The deciding officials are two senior DEA Special Agents who are responsible for assessing the discipline or punishment to be imposed.

## **Automated Systems**

During our 2002 audit we noted that DEA utilized separate systems for recording, tracking, and managing weapons and laptop computers. The DEA Weapons Database includes information on each weapon, including the make, model, serial number, name of the responsible custodian, location, acquisition date, and cost. Information on laptop computers is maintained in the DEA's Fixed Asset Subsystem, which contains laptop computer information such as asset number, serial number, manufacturer, model number, acquisition cost and date, name of the responsible Property Custodial Assistant, physical location, and condition.

### *Weapons*

In our 2002 audit report we reported that the DEA replaced its automated property management system for weapons (M-204 system) with a database system referred to by the DEA as the Weapons Database. As noted in our prior report, this change was necessary because the previous system contained unreliable information and had internal control weaknesses that allowed system users to manipulate data so that items in inventory could be transferred or deleted without approval. During the switchover to the new system, the DEA completed an inventory and reconciliation of all

---

<sup>19</sup> Personally Identifiable Information is any information about an individual, including, (but not limited to), education, financial transactions, medical history, criminal or employment history, or any information that can be used to distinguish or be traced to an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

DEA-owned weapons. In addition, one of the controls in the new firearms system is that only designated personnel in the Firearms Training Unit can access the Weapons Database.

### *Laptop Computers*

In our 2002 audit report we noted that the DEA had two automated systems comprising its official property management system for accounting for laptop computers: the Fixed Asset Subsystem and the Technical Equipment Inventory System. The Technical Equipment Inventory System recorded laptops used for technical purposes, such as surveillance and tracking. All other laptops were tracked in the Fixed Asset Subsystem.

During this follow-up review we found that the DEA is still utilizing dual systems to account for laptop computers. The Fixed Asset Subsystem allows field locations to change the status of laptops assigned to it to be "disposed of," "excessed," or "transferred," but does not allow a field office to access or change inventory data for other locations. The Technical Equipment Inventory System allows technical group supervisors in the field to issue laptops to users and update the status of laptop assignments. However, they are unable to delete information from the system. Dedicated inventory management specialists in the field are authorized to dispose of laptops with prior approval from the Office of Investigative Technology.

### **OIG Audit Approach**

We conducted this follow-up audit to assess the DEA's progress in addressing the weaknesses we identified during our previous audit regarding its control over weapons and laptop computers. Our review period for this follow-up audit covered the 66 months between January 2002 and June 2007.

We performed a complete inventory of all DEA weapons and laptop computers at DEA headquarters in Arlington, Virginia; the DEA warehouse in Alexandria, Virginia; the Special Operations Division and the Depot in Chantilly, Virginia; the Organized Crime Drug Enforcement Task Force Fusion Center in Merrifield, Virginia; and the DEA Training Academy in Quantico, Virginia. We also tested a statistical sample of weapons and laptop computers at the DEA field division offices in Chicago, Illinois; Denver, Colorado; Houston, Texas; Los Angeles, California; Miami, Florida; and New York, New York. Further, our audit included testing at these headquarters and field locations of the DEA's records and controls for its Special Agents authorized to carry personally owned weapons.

Our audit also examined the actions, including disciplinary and assessment of financial liability, taken in response to lost, stolen, and missing weapons and laptop computers as reported by the DEA Board of Professional Conduct. Additionally, we queried the NCIC to determine if lost, stolen, or missing weapons were entered into the system in a timely manner.

We also reviewed the DEA's internal controls over weapons and laptops, which included examining the accuracy and completeness of DEA records, evaluating the DEA's compliance with DOJ reporting requirements for lost or stolen items, and assessing the DEA's accountable property exit procedures for departing employees. We also tested a statistical sample of records for weapons and laptop computers that were disposed of at DEA headquarters and the Firearms Training Unit between January 1, 2002, and June 30, 2007. Additionally, our assessment of controls over weapons included physically verifying all weapons issued to Special Agents in the DEA headquarters geographic area and all stock weapons maintained at the Firearms Training Unit at Quantico, Virginia. We selected for testing 5,094 total weapons (4,331 DEA-owned and 763 personally owned) and 3,007 laptop computers.

#### ITEMS TESTED DURING OUR FOLLOW-UP AUDIT

Location	WEAPONS		LAPTOPS
	DEA Owned	Personally Owned	DEA Owned
DEA headquarters	388	189	2,189
Firearms Training Unit	3,322	0	554
Chicago	101	80	30
Denver	41	57	19
Houston	78	91	56
Los Angeles	171	91	59
Miami	102	131	39
New York	128	124	61
<b>TOTAL</b>	<b>4,331</b>	<b>763</b>	<b>3,007</b>

Source: OIG inventory of weapons and laptop computers at sites listed

In addition, where appropriate we compared results from this follow-up review of the DEA to results in our February 2007 follow-up audit report of the FBI's controls over weapons and laptop computers.<sup>20</sup> Our follow-up review of the FBI covered a 44-month period from February 2002 through September 2005. For this review, we computed and compared

<sup>20</sup> 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).

losses of weapons and laptops for these two agencies, and we comparatively evaluated the circumstances regarding losses.

This page intentionally left blank.

## FINDINGS AND RECOMMENDATIONS

### I. DEA'S RESPONSE TO WEAPON AND LAPTOP LOSSES

Since our 2002 audit the rate of loss for DEA laptop computers has decreased, but the rate of loss for weapons doubled from 0.61 to 1.37 weapons per month. Most important, the DEA was unable to provide assurance that the contents for 226 of 231 lost or stolen laptops did not contain sensitive information or personally identifiable information (PII). This is similar to the findings of our 2002 audit report. Additionally, while the DEA has improved some of its procedures relating to control and accountability for weapons and laptops since our previous audit, we found that the DEA did not correct several weaknesses identified in our 2002 audit. Specifically, the DEA did not timely and accurately report losses to appropriate DEA and Department officials and did not adequately ensure that lost property was entered in the NCIC database.

#### **DEA Lost or Stolen Weapons and Laptop Computers**

As shown in the following table, our 2002 audit of the DEA found that over a 26-month period 16 weapons and 229 laptop computers were lost or stolen, compared to 91 weapons and 231 laptop computers over a 66-month period in our follow-up audit. The DEA's average monthly rate of loss for weapons increased by 225 percent, while the rate of loss for laptop computers decreased by more than 50 percent.<sup>21</sup>

---

<sup>21</sup> Because the audit periods were different lengths, we analyzed the rate of loss on a monthly basis.

**DEA MISSING WEAPONS AND LAPTOP COMPUTERS  
2002 AUDIT COMPARED TO FOLLOW-UP AUDIT<sup>22</sup>**

Category	Number of Lost or Stolen Items Reported		Losses Reported Per Month	
	2002 Audit	Follow-up Audit	2002 Audit	Follow-up Audit
Lost Government Weapons	4	14	0.15	0.21
Lost Personal Weapons <sup>23</sup>	0	6	0	0.09
Lost Weapons, (unable to determine if government or personally owned)	0	2	0	0.03
Stolen Government Weapons	12	43	0.46	0.65
Stolen Personal Weapons	0	26	0	0.39
<b>Total Lost or Stolen Weapons</b>	<b>16</b>	<b>91<sup>24</sup></b>	<b>0.61</b>	<b>1.37</b>
<hr/>				
Lost Laptop Computers	229 <sup>25</sup>	206	8.81	3.12
Stolen Laptop Computers	0	25	0	0.38
<b>Total Lost or Stolen Laptops</b>	<b>229</b>	<b>231</b>	<b>8.81</b>	<b>3.50</b>

Source: OIG analysis of DEA Board of Professional Conduct case files

This table shows that the DEA made significant improvement in its rate of loss for laptop computers. Conversely, the DEA's average monthly rate of loss for weapons more than doubled from our previous audit.

We recognize that some weapons and laptops will inevitably be stolen or lost. However, it is important that the DEA take appropriate steps to minimize loss. Moreover, when losses occur, the DEA must report the losses promptly, both within the DEA and to DOJ. Further, the DEA must be able to identify the contents of laptops, determine whether the laptops are encrypted, and ensure weapons and laptops are entered into the NCIC database in a timely manner.

---

<sup>22</sup> Our review period for the 2002 audit covered 26 months, from October 1, 1999, to November 30, 2001. Our review period for the follow-up audit covered 66 months, from January 1, 2002, to June 30, 2007.

<sup>23</sup> Personally owned weapons authorized for official use were not tested in the 2002 audit.

<sup>24</sup> We were unable to determine whether these weapons were government owned or personally owned because the serial numbers were not in the file.

<sup>25</sup> The DEA reported that it could not account for 229 laptops during the prior audit. No detail was given as to the number of lost versus stolen.



We also compared the DEA and FBI rates of loss per employee, and found that the loss of weapons were similar. The FBI lost 3.49 weapons per 1,000 agents per year, while the DEA lost 3.36 weapons. For laptop computers, the FBI lost 3.49 per 1,000 agents per year compared to the DEA's rate of 8.52 laptops.

**DEA AND FBI MISSING WEAPONS AND LAPTOP COMPUTERS  
FOLLOW-UP AUDITS COMPARISON**

Component	Special Agents	Number of Months	Weapons		Laptops	
			Total Weapons Lost or Stolen	Weapons Lost or Stolen Per 1,000 Agents Per Year	Total Laptop Computers Lost or Stolen	Laptop Computers Lost or Stolen Per 1,000 Agents Per Year
DEA	4,929	66	91	3.36	231	8.52
FBI	12,515	44	160	3.49	160	3.49

Source: OIG analysis of DEA and FBI follow-up audit data

**Reporting Weapons and Laptop Computer Losses**

The DEA's Agent Manual requires the responsible employee to file a police report in the jurisdiction where the loss or theft of a weapon or laptop occurred. Additionally, the responsible employee or their immediate supervisor must ensure the weapon is entered in the NCIC database by the local police agency responsible for the jurisdiction in which the loss or theft was reported. Within 48 hours of the event, the responsible employee also must complete Part 1 of the DEA Form 29.

In October 2002 the DEA Administrator issued a memorandum requiring that all losses of laptop computers be reported within 48 hours of the incident to the DEA Board of Professional Conduct and the DEA Office of Professional Responsibility. The notification must include a full description of the laptop computer and circumstances surrounding the loss or theft. In addition, the notification must include a statement identifying whether the laptop contained any DEA sensitive or classified information.

The DEA Form 29 – Personal Property Negligence/Liability Assessment (see Appendix XI) is used to report within the DEA the loss or theft of a weapon or laptop. The form is required to be completed and signed by the employee and the employee's supervisor. The form is used to record pertinent information related to the loss, including information about the employee; the type of property; whether the property was DEA-owned, rented, or borrowed; whether the incident was reported to the police;

whether information on the property was entered into NCIC; and what happened to the property, such as was it lost, stolen, or damaged. Additionally, the form has an area to describe the item and an area for the employee to provide a statement regarding the events being reported. However, the form does not have a section for identifying the contents of the data stored on the laptop and whether the data included sensitive or PII. The form is also used to document the reporting office's results of the initial investigation of the incident and is then forwarded to the DEA Board of Professional Conduct.

The NCIC is a database of criminal justice information, including information on criminal record histories, fugitives, stolen property, and individuals incarcerated in the federal prison system. Criminal justice agencies throughout the United States enter records into NCIC, which are then accessible to law enforcement agencies nationwide. DEA policy requires that data regarding lost or stolen weapons and laptops be promptly entered into NCIC so that the information is available to law enforcement personnel while conducting enforcement functions. The DEA is a non-record entering agency for the NCIC, meaning DEA employees do not enter data into the system. Rather, the DEA relies on local law enforcement agencies to perform this task. However, failure to enter missing weapon and laptop data into the NCIC could result in reducing the chances of recovering the item or identifying the weapon if it is used in the commission of a crime.

Our 2002 audit found that DEA employees did not always report lost or stolen weapons and laptops to the DEA in a complete and timely manner and did not ensure that all lost or stolen weapons and laptops were entered into the NCIC database. As a result, we recommended that the DEA ensure all missing weapons and laptops were promptly entered into the NCIC database and reiterate to all employees the policy for reporting losses of DEA property as outlined in the DEA Agents Manual, Section 6122.13, Loss, Theft, or Destruction of a Firearm. In response to our 2002 audit recommendations, the DEA distributed DEA-wide teletypes on July 25 and August 22, 2002, reminding Special Agents of the requirements of the Agents Manual.

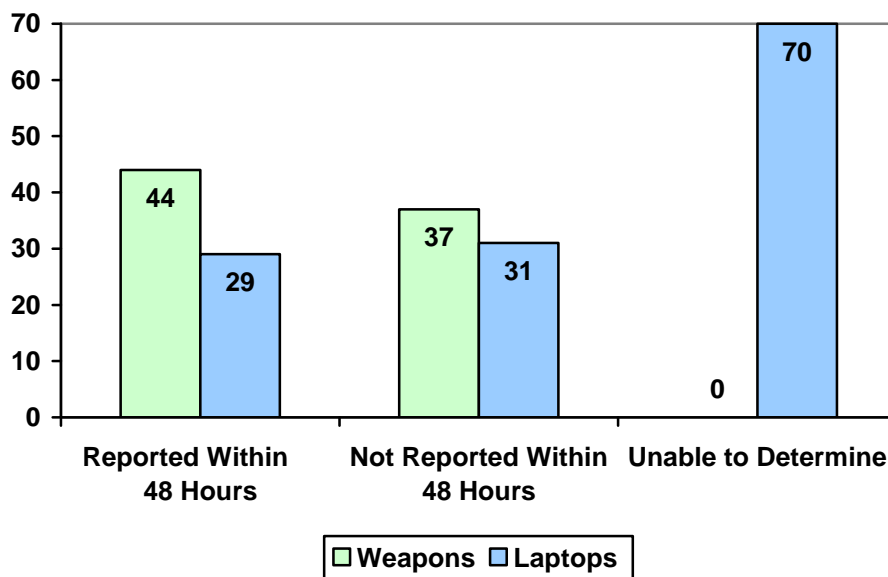
### *Reporting Weapon Losses*

During our follow-up audit, we reviewed the reporting actions taken by the DEA in response to lost or stolen weapons and laptop computers by examining DEA Forms 29 that were included as part of the DEA Board of Professional Conduct case files. The DEA was able to provide DEA Forms 29

for all 91 of the lost or stolen weapons. We also examined whether the losses were reported within 48 hours, entered into NCIC, and recovered.

The DEA prepared 81 DEA Forms 29 reporting the 91 missing weapons (7 forms included multiple weapons). We found that 37 (46 percent) of the forms were not completed within the required 48-hour timeframe. In 19 instances DEA personnel took over 2 weeks to report the loss, hindering a timely investigation regarding the circumstances of the loss. (Details on the number of days until losses were reported are contained in Appendix V.) In addition, 13 (16 percent) of the forms did not contain critical information, such as the correct serial number or whether the weapon was entered into NCIC. The failure of DEA to ensure that lost or stolen weapons were internally reported in a timely manner in accordance with DEA policy is a finding that we previously identified in our 2002 audit.

**TIMELINESS OF REPORTING LOST OR STOLEN WEAPON AND LAPTOPS  
DEA FORMS 29 SUBMITTED**



Source: OIG analysis of DEA Board of Professional Conduct case files

*Reporting Laptop Computer Losses*

We also examined 110 DEA Forms 29 for the 231 laptop computers reported missing.<sup>26</sup> For 70 of the 110 DEA Forms 29 (64 percent) we could

<sup>26</sup> Several cases reported multiple laptops on one DEA Form 29.

not determine if the forms were submitted within 48 hours as required by DEA policy because DEA personnel did not include submittal dates on the forms. We determined that 31 of the DEA Forms 29 (28 percent) were submitted late. Of these 31 forms, 20 were filed from 15 to over 1,700 days late, hindering timely investigation of the loss. We were able to determine that only 9 of the 110 DEA Forms 29 tested (8 percent) were submitted within the required timeframe. Appendix VI provides details on the number of days that laptops were reported late.

As mentioned previously, the DEA issued two teletypes in 2002 reminding Special Agents of policy regarding reporting losses of property. However, our audit results indicate that the DEA did not ensure that its staff was filing reports for lost or stolen property within the required 48 hours. DEA management needs to ensure that its staff prepares complete and accurate loss reports and submits those reports to the appropriate offices in a timely manner.

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

Our review of the DEA Board of Professional Conduct case files found that only 5 of the 231 lost or stolen laptop computers contained information regarding the sensitivity of the contents of the missing laptops.

For the other 226 laptops reported lost or stolen during our review period, we asked the DEA Board of Professional Conduct Chairman, Office of Professional Responsibility Deputy Chief Inspector, and Office of Security Programs Information Security Section Chief what the DEA did to determine the contents of the other lost or stolen laptop computers. In response, the DEA provided the following statement:

DEA is unable to provide, with certainty, assurance that the content of many of these laptops is not sensitive information because it does not remotely (in an automated manner) manage its laptops. The majority of DEA's laptop computers are used as standalone computing devices. DEA's policy prior to 2007 (Asa Hutchinson's October 2002 Memo) did not allow sensitive data or classified information to be processed on standalone laptops. During the time prior to the PII mandate in July 2006, DEA asked only for affirmation from users that no sensitive or classified data was on the missing devices. After 2007, sensitive data was authorized to be processed on laptops that have full hard-disk encryption.

In addition to this statement, the DEA Security Programs Information Security Section Chief told us that DEA investigators attempt to determine what information may have been lost or compromised, but said there is no way to determine the contents of the missing laptop unless it is recovered. However, we found no evidence that this was done for the most of the laptops.

We asked the DEA to provide the results of any investigations it conducted to determine the contents of the 231 lost or stolen laptop computers. In response, the Office of Security Programs Information Security Section Chief was only able to provide results regarding three lost or stolen laptop computer cases. He stated that in one case the laptop contained sensitive information but was fully encrypted. In another case, the laptop was not encrypted, but did not contain Personally Identifiable Information. In the third case, the missing laptop did not contain sensitive information but did contain contract information.<sup>27</sup> Because the DEA could not provide serial numbers for these three laptops, we could not determine whether they were part of the 231 lost or stolen laptops identified during our follow-up audit or whether these were additional losses.

In addition, since October 2002 the DEA has required that reports of lost or stolen laptops must include a statement identifying whether the laptop contained any DEA sensitive or classified information. We did not find any of these required statements in the DEA Board of Conduct case files for 226 laptops identified as lost or stolen. As a result, the DEA could not provide assurance that the laptops did not contain sensitive or PII information.

The DEA was able to confirm the contents for five of the lost or stolen laptops. Of the five, one was determined by the DEA to contain sensitive case information while the remaining four did not.

In our opinion, the DEA failed to adequately determine the contents of the lost and stolen laptops. We believe the DEA must implement policies to ensure that it identifies the contents of any lost or stolen laptops and whether these laptops contained sensitive, classified, or personally identifiable information.

---

<sup>27</sup> DOJCERT assists in handling computer security incidents throughout DOJ. DOJ regulations require all components to submit immediate reports summarizing incidents involving the loss of both classified and unclassified systems to DOJCERT. DOJCERT maintains a database of reported incidents. The DEA's lack of reporting to DOJCERT is discussed in Finding II.

## *Encryption of Laptop Computers*

DEA reported that as of December 2007, 155 of the DEA's 3,548 laptops that required encryption were not yet encrypted. Of the DEA's 5,287 laptops, 1,739 were not authorized to contain sensitive information and according to DEA policy do not require encryption. In our judgment, due to the sensitivity of the data that DEA generally processes, we believe the DEA should revise its policy to ensure that all laptop computers are encrypted to minimize the risk of loss of sensitive DEA data.

As shown in the following table, 64 percent of DEA's laptop computers had been encrypted as of December 2007.<sup>28</sup> Of the 36 percent of laptops that were not encrypted, the DEA reported that 3 percent were in the process of being encrypted and the remaining 33 percent were exempt for encryption because they were not used to process sensitive information. According to a DEA policy, effective July 30, 2007, 1,739 laptops (33 percent) are used by Special Agents or Investigative Technology Specialist to support electronic surveillance, computer forensics, polygraph examinations and other digital monitoring functions.

**DEA LAPTOP COMPUTERS ENCRYPTED**  
**Laptops in Use as of December 2007**

Category	Number	Percent
Encrypted	3,393	64%
Exempt	1,739	33%
In Progress <sup>29</sup>	155	3%
<b>Total</b>	<b>5,287</b>	<b>100%</b>

Source: OIG analysis of DEA Security Information Office data

During our fieldwork, we attempted to determine whether DEA laptops in the field offices we visited were encrypted and what data was contained on the laptops. As shown in the following table, we found that 79 of

---

<sup>28</sup> On March 28, 2007, the DEA submitted a memorandum to the DOJ Chief Information Officer requesting a 60-day extension, to May 31, 2007, for meeting the DOJ requirement to ensure that all unclassified laptops had encryption to protect sensitive data. This memorandum noted that the DEA began encrypting laptop computers in mid-November 2006. The DOJ Chief Information Officer approved the DEA's request. According to DEA policy implemented on July 30, 2007, all laptop computers used to process sensitive information must be encrypted.

<sup>29</sup> DEA officials informed us that these laptops were assigned to personnel in temporary duty status, have compatibility issues with the encryption software, require additional memory, or need batteries.

164 laptops we examined were not encrypted. Of the 79 unencrypted laptops, we identified at least 5 that contained sensitive or personally identifiable information. In addition, the password and user ID for one of the encrypted laptops was attached to the laptop.<sup>30</sup>

**NUMBER OF LAPTOPS TESTED**

<b>Field Office</b>	<b>Reviewed</b>	<b>Encrypted</b>	<b>Not Encrypted</b>
Chicago	23	13	10
Denver	18	11	7
Houston	33	13	20
Los Angeles	47	5	42
Miami	17	17	0
New York	26	26	0
<b>Total</b>	164	85	79

Source: OIG analyses of laptops tested

*Entering Losses into NCIC*

DEA policy specifies that all lost or stolen personal property, including laptops, is required to be entered into NCIC. During our 2002 audit we found that the DEA did not ensure that all lost or stolen weapons were entered into the NCIC database. Specifically, we determined that 6 of the 16 lost or stolen weapons (38 percent) were not entered into the NCIC database. In this follow-up audit, we reviewed DEA loss documentation and queried the NCIC database for the 91 lost or stolen weapons. We found that 11 weapons were not entered in the NCIC database, and 7 weapons were entered with incorrect serial numbers. Serial numbers uniquely identify a weapon, and incorrect serial numbers will likely prevent an NCIC user from matching a weapon to one cataloged inaccurately in the NCIC database. We determined that 17 of the 73 weapons correctly entered in the NCIC database were recovered. Appendix VII provides details on the weapons that were not found in the NCIC database.

We determined that only two DEA Forms 29 contained enough information to show that the laptop was entered into the NCIC. There was not enough information on the DEA Forms 29 to confirm whether 229 of the 231 lost or stolen laptop computers were entered into NCIC. We queried the

---

<sup>30</sup> Our review of the contents of laptops at the field sites visited consisted of a visual inspection of the programs and recently modified files contained on the laptops. Our review did not examine the entire contents of the laptops.

NCIC database for the lost or stolen laptops and found that 229 laptops did not have a record in the NCIC database.

Promptly and accurately entering information on lost and stolen weapons and laptops can assist in recovering the missing property. However, the DEA Agents Manual does not include policy pertaining to internal reporting procedures for lost or stolen laptops, including entering relevant information in the NCIC database. We believe the DEA should include procedures for reporting lost or stolen laptop computers in the manual. Further, DEA management should be required to ensure that all lost or stolen weapons and laptops have been accurately entered in the NCIC database.

Overall, we believe that the DEA still needs significant improvement in its internal reporting of lost and stolen weapons and laptop computers and in entering laptop losses into the NCIC database. Comparing our results of the DEA from this audit with those of our FBI follow-up audit, we found that the DEA and FBI were similarly poor in internally reporting weapons and laptop losses and in entering laptop losses in the NCIC database. The following table provides details of our comparison.

**COMPARISON OF DEA AND FBI REPORTING  
OF LOST OR STOLEN WEAPONS AND LAPTOPS**

	DEA					FBI				
	YES	NO	Unable to Determine	Total	Percent Yes	Yes	NO	Unable to Determine	Total	Percent Yes
Weapon Loss Reported Timely	31	37	13	81	38%	52	54	51	157	33%
Weapons Entered into NCIC	73	18	0	91	80%	137	23	0	160	86%
Laptop Loss Reported Timely	9	31	70	110	8%	16	38	106	160	10%
Laptops Entered into NCIC	2	216	13	231	1%	24	136	0	160	15%

Source: OIG FBI Follow-up audit and OIG analysis of the DEA Board of Professional Conduct files

**Referring and Investigating Losses**

Our 2002 audit found that DEA lost or stolen weapons were reported and investigations were initiated on all 16 instances of loss. However, our



previous audit also found that the DEA could not account for 229 laptops in an agency-wide reconciliation of its property inventory. In our previous audit we were also unable to test whether the DEA's policies and procedures concerning lost or stolen laptop computers were adequate because DEA was unable to provide reliable data. Therefore, we could not determine how many lost or stolen laptop computers were reported and referred to the DEA Office of Professional Responsibility for investigation.

The DEA issued interim policy on March 30, 2007, designating the DEA Office of Professional Responsibility as the unit with the overall management of the DEA Lost or Stolen Firearm Program. The policy authorizes the Office of Professional Responsibility to determine whether it will investigate the case or refer it to the reporting office for investigation. If the case is referred to the reporting office, the office head must assign the matter for investigation to a Special Agent or Diversion Investigator who is a grade equal to or higher than the grade of the responsible employee and who is not directly associated with the responsible employee. The investigation should verify the facts and circumstances surrounding the loss, theft, or destruction as reported by the responsible employee. The investigation also should acquire facts necessary to determine whether the property was being used in an official capacity and whether personal negligence contributed to the loss or theft. According to DEA policy, a completed Report of Investigation must be submitted to the DEA Board of Professional Conduct within 30 days of the loss, theft, or destruction

As previously noted, in October 2002 the DEA Administrator issued a memorandum requiring laptop computer losses to be reported to the DEA Board of Professional Conduct and the DEA Office of Professional Responsibility within 48 hours of the incident. However, the DEA Board of Professional Conduct Chairman told us during our current audit that not all lost or stolen weapon and laptop cases have been referred for investigation to the DEA Office of Professional Responsibility. Weapons and laptops that were reported by the DEA field offices as lost or stolen were only referred by the Board of Professional Conduct to the Office of Professional Responsibility if documentation presented in the report indicated some form of misconduct was involved in the loss, theft, or destruction of the weapon or laptop.

The following table summarizes the total number of lost or stolen weapons and laptop computers that were referred to the Office of Professional Responsibility for investigation.

**REFERRALS AND INVESTIGATIONS OF  
WEAPON AND LAPTOP LOSSES**  
January 1, 2002, through June 30, 2007

Category	Referred to the DEA Office of Professional Responsibility	Not Referred to the DEA Office of Professional Responsibility	Unable to Determine Whether Referred to the DEA Office of Professional Responsibility	Total Number of Lost or Stolen Items
Lost Weapons	14	8	0	22
Stolen Weapons	40	10	19	69
<b>Total Lost or Stolen Weapons</b>	<b>54</b>	<b>18</b>	<b>19</b>	<b>91</b>
Lost Laptop Computers	1	0	205	206
Stolen Laptop Computers	1	0	24	25
<b>Total Lost or Stolen Laptops<sup>31</sup></b>	<b>2</b>	<b>0</b>	<b>229</b>	<b>231</b>

Source: OIG analysis of DEA Board of Professional Conduct Case Files

### **Disciplining Employees Responsible for Losses**

In the case of a lost or stolen weapon or laptop, the DEA Office of Professional Responsibility determines whether it will investigate the case or refer it to the reporting office for investigation. As stated previously, the Office of Deciding Officials assesses disciplinary action as deemed appropriate.

#### *Weapon Loss*

Our follow-up review of the DEA Board of Professional Conduct case files found instances when losses occurred despite reasonable precautions taken by DEA employees. However, we also found instances of lost or stolen weapons resulting from employees' carelessness or failure to follow DEA policy. For instance, the DEA Agents Manual, Section 6122.42 Firearms Security, Safety and Storage, specifically states that DEA issued and authorized personally owned weapons may not be left unattended or temporarily stored in an official government or privately owned vehicle. As shown in the following table, we found that 44 of the 69 stolen weapons (64 percent) were stolen from official government or privately owned vehicles. The weapons stolen included pistols, rifles, shotguns, and a submachine gun. Pistols accounted for 39 of the 44 weapons stolen from

---

<sup>31</sup> A total of 231 laptops were lost or stolen for 110 cases filed.

vehicles (89 percent). Further details of these losses are provided in Appendix III.

**WEAPONS REPORTED LOST AND STOLEN BY TYPE  
JANUARY 1, 2002, THROUGH JUNE 30, 2007**

	Pistol	Shotgun	Rifle	Submachine Gun	Total Weapons
<b>Lost:</b>					
Inventory	4	0	0	0	4
Miscellaneous <sup>32</sup>	15	2	0	1	18
<b>Subtotal</b>	<b>19</b>	<b>2</b>	<b>0</b>	<b>1</b>	<b>22</b>
<b>Stolen:</b>					
From Official Government Vehicle	31	2	2	1	36
From Privately Owned Vehicle	8	0	0	0	8
From Residence	13	0	0	0	13
Other <sup>33</sup>	11	1	0	0	12
<b>Subtotal</b>	<b>63</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>69</b>
<b>Total</b>	<b>82</b>	<b>5</b>	<b>2</b>	<b>2</b>	<b>91</b>

Source: OIG analysis of the DEA Board of Professional Conduct case files

Comparing the DEA follow-up audit results of lost and stolen weapons with the follow-up audit results of the FBI, we found that the DEA and FBI both experienced weapons being stolen from government owned and privately owned vehicles in relatively similar rates. DEA had 44 weapons stolen from vehicles while the FBI had 58 weapons stolen from vehicles. We found that the DEA and FBI had 1.62 and 1.26 weapons stolen from vehicles per 1,000 agents per year, respectively.

We reviewed the DEA Board of Professional Conduct files to determine the actions taken for the 91 weapons that were lost or stolen. Although 91 weapons were reported as lost or stolen, multiple weapons were included

---

<sup>32</sup> These weapons were lost under a variety of circumstances. For example, one weapon was left on top of a Special Agent's car and presumably lost as he drove off. One weapon was destroyed in a bombing and another was destroyed in a fire.

<sup>33</sup> These weapons were stolen under a variety of circumstances. For example, one weapon was stolen from a boat loading dock where it was left unattended. Another was placed in a briefcase and left behind in a restaurant.

in 7 cases; therefore, 81 actions were taken on these losses. The DEA's reviews resulted in the following 81 actions:

- 26 instances resulted in no disciplinary action;
- 46 instances resulted in suspensions of the responsible employees, ranging from 1 to 7 days;
- 1 instance resulted in suspension of the responsible employee for 30 days;
- 5 instances resulted in the employees receiving a Letter of Caution; and
- 3 instances resulted in the employees receiving a Letter of Reprimand.

We found that all 91 weapon losses were investigated by DEA Special Agents where the loss or theft occurred and referred to the Board of Professional Conduct as required by DEA policy. We also found that the disciplinary actions taken by the DEA appeared to be consistently imposed.

#### *Laptop Computer Loss*

Similar to the reports of lost and stolen weapons, many laptop computer losses could have been avoided if employees were more careful and complied with DEA policies. For example, one laptop was left in a taxi and another was stolen from checked luggage. As shown in the following table, the DEA could not provide the circumstances of the losses for 206 of 231 missing laptop computers (89 percent). These laptops were discovered missing during routine inventories and other unexplained circumstances. After our initial testing, the DEA was able to locate or find supporting documentation that accounted for 8 of the 206 missing laptops. The DEA identified 149 of these 206 laptops as missing (72 percent) when conducting annual laptop inventories. In addition, 4 laptops were lost after being left unattended and 26 laptops were believed to have been disposed of or transferred, but no supporting documentation was available to substantiate this claim. The DEA was unable to determine the circumstances of the loss for an additional 27 laptops. The remaining 25 laptop computers (11 percent) were reported as stolen from vehicles and other locations. Appendix IV includes more detail on reported laptop losses.

**LAPTOP COMPUTERS REPORTED LOST AND STOLEN  
January 1, 2002, through June 30, 2007**

Total	
<b>Lost:</b>	
Inventory	149
Left Unattended	4
No Documentation	26
Unknown	27
<b>Subtotal</b>	<b>206</b>
<b>Stolen:</b>	
From Official Vehicle	8
From Residence	1
Other <sup>34</sup>	16
<b>Subtotal</b>	<b>25</b>
<b>Total</b>	<b>231</b>

Source: OIG analysis of DEA Board of Professional Conduct case files

As shown in the following table, the DEA and FBI follow-up audit results for stolen laptop computers, we found that the DEA and FBI both averaged nearly 1 stolen laptop computer per 1,000 agents per year. We also noted that the DEA had 8 laptops stolen from official vehicles while the FBI had 23 laptops stolen in such a manner. The DEA averaged 0.30 laptops stolen from vehicles per 1,000 agents per year, compared to the FBI's rate of 0.50 laptops.

**FOLLOW-UP AUDIT COMPARISON OF  
DEA AND FBI LAPTOP COMPUTERS STOLEN AND  
LAPTOP COMPUTERS STOLEN FROM VEHICLES**

Component	Special Agents	Number of Months	Total Laptops Stolen	Laptops Stolen Per 1,000 Agents Per Year	Total Laptop Computers Stolen From Vehicles	Laptop Computers Stolen From Vehicles Per 1,000 Agents Per Year
DEA	4,929	66	25	0.92	8	0.30
FBI	12,515	44	44	0.96	23	0.50

Source: OIG analysis of DEA and FBI follow-up audit data

<sup>34</sup> These laptop computers were stolen under a variety of circumstances. For example, several laptops were reported stolen from hotels and temporary quarters. Another laptop was reported stolen from checked luggage.

We reviewed the DEA Board of Professional Conduct files to determine the actions taken for the 231 laptop computers that were lost or stolen. In several instances, multiple laptops were reported on a single DEA Form 29. We found that the 206 lost laptop computers resulted in 85 Board of Conduct cases. The DEA's reviews of laptop losses resulted in the following 85 actions.<sup>35</sup>

- Seventy-three instances involved no disciplinary action.
- Two instances resulted in the responsible employees receiving a Letter of Reprimand.
- Ten instances resulted in the responsible employees receiving a Letter of Caution.

We also determined that each of the 25 stolen laptops was a separate Board of Conduct case and that the following actions were taken:

- Eleven instances involved no disciplinary action.
- Eight instances resulted in the responsible employee receiving a Letter of Reprimand.
- Four instances resulted in the responsible employee receiving a Letter of Caution.
- Two instances resulted in the responsible employee receiving suspensions, one for 2 days the other for 3 days.

We found that all 231 laptop losses were referred to the Board of Professional Conduct as required by DEA policy, and that disciplinary actions taken by the DEA appeared to be administered consistently. For 226 laptops, we found that the DEA was unable to determine if the laptops contained sensitive case information or PII. However, for five laptops the DEA was able to determine the laptops' contents and one of the five contained sensitive case information.

---

<sup>35</sup> Several DEA Forms 29 reported multiple lost or stolen laptops on a single form.

## **Conclusion**

Our follow-up audit found that the DEA decreased its rate of loss for laptop computers since our 2002 audit by more than 50 percent. In our 2002 audit report, we reported that the DEA could not determine if any of the lost, missing, or stolen DEA laptop computers resulted in a compromise of investigative information. In this audit we found that the DEA still could not determine what was on its lost or stolen laptops. We found that for 226 of the 231 lost or stolen laptops reported in our follow-up audit review period the DEA is unable to provide any assurance that the lost or stolen laptops did not contain sensitive information. In addition, we found that the DEA did not install encryption software on all of its laptop computers.

We found in this audit that the loss rate for weapons more than doubled from 0.61 to 1.37 per month since our last review. We also determined that 48 percent of the stolen weapons resulted from employees' carelessness or failure to follow DEA policy because Special Agents left weapons in either government or personally owned vehicles.

In addition, the DEA was not ensuring that lost or stolen weapons and laptops were entered in the NCIC database as required by DEA policy. We also found that 46 percent of the Form 29s were not prepared in a timely manner. These findings mirror weaknesses that we identified in our 2002 audit.

## **Recommendations**

We recommend that the DEA:

1. Ensure that all DEA Forms 29 submitted are complete, accurate, and promptly submitted in accordance with DEA policy.
2. Ensure that weapon and laptop computer losses are accurately and promptly entered into the NCIC database.
3. Revise the DEA Agent Manual to include procedures for actions required by DEA personnel to report lost or stolen laptop computers. At a minimum the Agent Manual should be revised to require information on laptop make, serial number, model number, NCIC record number, and a statement on the contents of the laptop and whether it contained classified, sensitive, or PII. The DEA Agent Manual should also be revised to require that the investigation of lost

or stolen laptops verify the contents of any missing laptop and ensure this information is described in detail in the case files.

4. Revise its policy to ensure that all laptop computers are encrypted.



## **II. INTERNAL CONTROLS**

In our 2002 audit we reported that the DEA had significant internal control weaknesses to account for and prevent losses of property such as weapons and laptops. This follow-up audit found that the DEA has improved its controls and procedural compliance in some areas, such as conducting physical inventories annually and ensuring adequate segregation of duties for personnel conducting inventories, performing reconciliations, and modifying the inventory system. However, we identified continued control weaknesses in several other areas. Specifically, the DEA failed to adequately maintain documentation for laptop disposals, did not report weapon and laptop computer losses to DOJ as required, and did not institute procedures to consistently ensure the return of laptop computers from separating employees.

Internal controls relevant to accountable property management are intended to provide reasonable assurance that resources are adequately safeguarded and efficiently used and that reliable data is maintained and properly reported. Management of an agency is responsible for the design, implementation, and maintenance of internal control procedures. For this audit we tested the DEA's internal controls over weapons and laptops by assessing its internal control structure and its compliance with procedures for conducting inventories, maintaining sufficient and accurate property records, reporting incidents of loss to the DOJ, accounting for the disposal of property, and ensuring exiting employees remit DEA-issued property.

### **Physical Inventories**

DEA's regulations require an annual inventory of all weapons and laptop computers. In our 2002 audit report we noted that the DEA did not perform annual physical inventories of all weapons, and the duties for maintaining records of weapons were not appropriately segregated within the Firearms Training Unit. We recommended that the DEA ensure that it conducts annual physical inventories of weapons and adequately segregates the duties of staff who conduct these inventories, perform reconciliations, and modify the inventory system. We also recommended that the DEA ensure that a valid inventory is available to all Property Custodial Assistants.

During our follow-up audit we reviewed DEA-wide inventory reports for fiscal years 2002 through 2006. We noted that DEA completed annual

physical inventories of its weapons and laptop computers. Additionally, we found that duties related to weapons inventory were adequately segregated within the Firearms Training Unit. We also found that a valid inventory was made available to all Property Custodial Assistants.

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

In our 2002 audit report we determined that the DEA's financial system was not integrated with its weapons inventory system, which would help ensure inventory accuracy, and the financial system did not include an audit function that allowed edits made to the Weapons Database to be tracked by an automated exception report. We recommended that the DEA develop internal controls, operating manuals, audit trails, and appropriate system requirements to ensure the reliability of inventories in its weapons inventory system – the Weapons Database. In addition, DEA's financial system was not fully integrated with the Fixed Asset Subsystem. As a result, the systems did not automatically verify whether the number of laptops actually purchased agreed with the number of items placed into inventory. We also recommended that the DEA integrate the financial system and the Fixed Asset Subsystem so that the inventory is routinely updated when a laptop computer is purchased.

In response to our recommendations, the DEA implemented the following internal controls:

- Entry capability for the Weapons Database is restricted to and appropriately segregated within the Firearms Training Unit.
- Field components are provided with their respective inventories for reconciliation purposes quarterly.
- The accuracy of the Weapons Database is verified quarterly by Primary Firearm Instructors and annually through a physical inventory.

The DEA's financial system still has not been integrated with the Weapons Database. However, based on our testing of the DEA's internal controls related to the Weapons Database, we consider the control procedures instituted by the DEA to be sufficient for ensuring that information in the Weapons Database is accurate, complete, and reliable.

## *Weapons*

We confirmed that entries into the Weapons Database are restricted to the Firearms Training Unit staff, and we found these duties were segregated within the unit to provide the DEA increased control over its weapons. We also tested the DEA's accounting of purchased weapons by comparing purchase documents to inventory data in the Weapons Database for the period of October 1, 2005, through February 28, 2007. Our testing included verifying the name of the manufacturer, serial number, model number, and caliber. We examined 7 bulk weapons purchases totaling 525 weapons, and we did not identify any discrepancies between the information on the purchase records and in the Weapons Database.

## *Laptops*

We determined that the financial system has been fully integrated with the Fixed Asset Subsystem used to maintain laptop computer inventories, and the DEA has implemented policy requiring properly segregated duties of staff conducting physical inventories, performing reconciliations, and modifying the property management system.

We tested the DEA's accounting for all DEA laptop computer purchases from October 1, 2005, through February 28, 2007. Our testing included verifying purchase records to laptop inventory records maintained in the Fixed Asset Subsystem, including the name of the manufacturer, serial number, and DEA number. In total, we tested 1,056 laptop purchases. In this testing, we were unable to trace the purchase documentation to Fixed Asset Subsystem inventory records for 68 laptops (6 percent) because:

- no documentation was available for 8 purchased laptops;
- 9 purchased laptops were not found in the inventory provided; and
- insufficient documentation was provided for 51 purchased laptops.

Further, during our testing, the DEA was unable to provide the OIG with requested purchase documentation in a reasonable amount of time because the purchase documentation for laptops is not maintained at a centralized location. In order to complete our testing we had to request that the applicable field office provide the required supporting documentation. In this effort, we had to make numerous requests of some field offices to

provide the supporting purchase documentation or to provide sufficient documentation to allow us to verify the laptop with the inventory system data. These delays and the 68 laptops not in the DEA inventory system indicate a need for better controls over laptop inventory records. We believe the DEA should retain copies of all disposal documentation at centralized locations in each division office to manage the program more effectively, enable quicker reconciliations, and provide adequate audit trails.

### **Accuracy and Completeness of Property Records in the Weapons Database and Fixed Asset Subsystem**

In our 2002 audit we selected a sample of weapons and laptop computers from these systems and physically verified their existence. Also in our 2002 audit, the DEA was able to provide all sampled weapons and laptop computers for our physical verification.

During our follow-up audit we tested the accuracy and completeness of the Weapons Database and Fixed Asset Subsystem. To perform this testing we selected samples of weapons and laptops and conducted physical verifications to assess the completeness and accuracy of DEA inventories.

#### *Weapons*

To perform our testing of the accuracy and completeness of the DEA's weapons inventory, we selected for verification purposes samples of DEA assigned weapons. Our testing included all of the unassigned stock weapons stored in the armory at the DEA Firearms Training Unit and stock weapons maintained at DEA headquarters for the Foreign-deployed Advisory Support Teams.<sup>36</sup> In addition, we verified all DEA-owned weapons assigned to DEA Special Agents in DEA headquarters' offices and in DEA field offices that we visited. We also tested personally owned weapons that Special Agents were authorized to carry for official duty at these same locations.

In total, we tested 4,331 DEA-owned and 763 personally owned weapons. We were able to verify the existence of 4,320 (99.7 percent) DEA-owned weapons and all 763 of the personally owned weapons tested. We considered that the DEA presented the weapon if it was able to

---

<sup>36</sup> According to the DEA, the Foreign-deployed Advisory Support Teams are comprised of DEA Special Agents and Intelligence Research Specialists that provide guidance and conduct bilateral investigations to identify and dismantle illicit drug trafficking and money laundering organizations in Afghanistan.

physically produce the weapon or appropriate documentation supporting that the weapon existed or had been subsequently lost, stolen, destroyed, or surplused after the draw date for our statistical sample. The following table details our testing.

#### WEAPONS TESTED AND VERIFIED

Location	DEA Owned		Personally Owned	
	Tested	Verified	Tested	Verified
DEA headquarters	388	388	189	189
Firearms Training Unit	3,322	3,321	0	0
Chicago	101	94	80	80
Denver	41	41	57	57
Houston	78	78	91	91
Los Angeles	171	168	91	91
Miami	102	102	131	131
New York	128	128	124	124
<b>TOTALS</b>	<b>4,331</b>	<b>4,320</b>	<b>763</b>	<b>763</b>

Source: OIG inventory of DEA weapons

Overall, our testing revealed that the DEA's inventory records for DEA-owned weapons were generally complete and accurate. For the 11 weapons that we could not verify, the DEA provided the following reasons for being unable to produce the weapons.

- For seven weapons originally located at the Chicago field division office, the DEA believes, and the DEA Weapons Database indicated, that the weapons were destroyed. However, the DEA could not provide documentation to substantiate the destruction.
- Two weapons were assigned to Special Agents from the Los Angeles Field Division. These agents were on special assignments outside the division, and therefore their weapons could not be physically verified.
- We determined that one weapon from our sample was an erroneous entry in the Weapons Database. The weapon could not be tested because the DEA never actually purchased the weapon.
- One non-functional training weapon located at the Firearms Training Unit could never be located.

We also tested DEA records to ensure appropriate authorization was documented for DEA personnel carrying personal firearms on official duty.

All DEA Special Agent personally owned weapons that we tested had appropriate approvals for carrying the firearm in an official capacity. We also verified that the weapons presented by the Special Agents were the weapons named in the authorizations.

*Laptop Computers*

In addition to performing verification testing of weapons, we conducted similar testing on a sample of DEA laptop computers. Our sample consisted of 3,007 of the DEA's 7,381 total laptop computers. Similar to our weapons testing, our sample of laptops included all laptops assigned to DEA headquarters entities and the Firearms Training Unit as well as a statistical sample of laptops assigned to the field offices where we performed our fieldwork. We considered that the DEA had accounted for the laptop if it was able to present the laptop for our verification or provide documentation supporting that the laptop existed. We also accepted documentation supporting that the laptop was lost, stolen, destroyed, or surplused after the date our statistical sample was selected.

As shown in the following table, the DEA was able to account for 2,965 (99 percent) of the 3,007 laptops in our sample. The DEA was unable to provide adequate supporting documentation to confirm that 42 laptops (1 percent) assigned to DEA headquarters locations had not been either lost or stolen. In addition, we found that 20 had not been entered into the Fixed Asset Subsystem. The DEA took immediate corrective action after we brought this to their attention by adding these 20 laptops to its inventory in the Fixed Asset Subsystem.

**LAPTOP COMPUTERS TESTED AND VERIFIED**

<b>Location</b>	<b>Tested</b>	<b>Verified</b>
DEA headquarters	2,189	2,147
Firearms Training Unit	554	554
Chicago	30	30
Denver	19	19
Houston	56	56
Los Angeles	59	59
Miami	39	39
New York	61	61
<b>TOTALS</b>	<b>3,007</b>	<b>2,965</b>

Source: OIG inventory of DEA laptop computers

**Reporting Losses to DOJ**

Besides internal DEA reporting procedures discussed in Finding I that require DEA employees to report lost or stolen weapons and laptops to the

DEA in a complete and timely manner. DOJ also requires all components to submit to the DOJ Justice Management Division semiannual reports on January 1 and July 1 summarizing the loss or theft of government property that occurred within the preceding 6 months.<sup>37</sup> In our 2002 audit we found that the DEA did not submit any semiannual Department Theft Reports for 1999 and 2000, and the first semiannual report for 2001 was submitted 36 days late. In addition, the semiannual reports were inaccurate with respect to the number of weapon losses. We recommended that the DEA submit timely and complete semiannual Department Theft Reports to the DOJ.

In this follow-up audit we again examined the DEA's submission of semiannual Department Theft Reports. Additionally, we also analyzed in this audit the DEA's compliance with the DOJ regulations requiring all components to immediately notify the DOJCERT of incidents involving the loss of laptops. Properly reporting losses to the DOJ helps maintain the DEA's accountability during incidents of loss. Additionally, it assists in recovering losses and mitigating any adverse impact, such as when losing a laptop with sensitive information.

#### *DOJ Semiannual Reports*

Our follow-up review found that the DEA has not corrected its deficiency in reporting to the DOJ on the weapons and laptop computers that were lost or stolen during semiannual periods. During the time period our audit covered, 11 semiannual Department Theft Reports were supposed to be submitted to the DOJ. However, the DEA was only able to provide, and DOJ only had on file, three semiannual reports (January 1 to June 30, 2005; June 1 to December 31, 2006; and January 1 to June 30, 2007). The DEA did not submit semiannual reports for all of 2002 through 2004; July 1 to December 31, 2005; and January 1 to May 31, 2006.

We also reviewed the three Department Theft Reports submitted by the DEA during our audit period and found that only one report was complete and accurate. The report for the period ending December 31, 2006, did not report as many weapons and laptops missing as compared to the files we reviewed at the Board of Professional Conduct. The report for the period ending June 30, 2007, did not report any weapons missing even though DEA records showed four weapons were reported lost during the

---

<sup>37</sup> See DOJ Order 2630.2A, Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures.

previous 6 months. The reports for the periods ending December 31, 2006, and June 30, 2007, were submitted in a timely manner. However, we were unable to determine if the report for the period ending June 30, 2005, was submitted when required. When we asked about the eight missing reports, the Deputy Assistant Administrator, Office of Administration, told us that the administrative clerk responsible for preparing the semiannual theft reports typed over the prior reports and failed to maintain a paper or electronic copy of the reports.

During the period of January 1, 2002, through June 30, 2007, 87 weapons and 200 laptops should have been reported to the DOJ on semiannual Department Theft Reports. As shown in the following table, DOJ was not aware of 67 weapons and 176 laptops that were lost or stolen because the DEA did not submit to the DOJ Justice Management Division the required semiannual Department Theft Reports. Therefore, only 20 weapons (23 percent) and 24 laptops (12 percent) were reported to the Justice Management Division as required by DOJ regulations.

**ACCURACY OF DEA'S SEMI ANNUAL REPORTS TO DOJ**  
**Semiannual Reports due June 30, 2002 through June 30, 2007**

Semiannual Period Ended	Weapon Losses			Laptop Losses		
	DEA Records	Reported to DOJ	Not Reported to DOJ	DEA Records	Reported to DOJ	Not Reported to DOJ
06/30/02	4		4	11		11
12/31/02	12		12	62		62
06/30/03	10		10	20		20
12/31/03	6		6	52		52
06/30/04	6		6	11		11
12/31/04	12		12	9		9
06/30/05	8	18	(10)	3	6	(3)
12/31/05	15		15	13		13
06/30/06	6		6	2		2
12/31/06	4	2	2	14	8	6
06/30/07	4		4	3	10	(7)
<b>Total</b>	<b>87</b>	<b>20</b>	<b>67</b>	<b>200</b>	<b>24</b>	<b>176</b>

Source: OIG analysis of DEA Board of Professional Conduct case files and semiannual reports



## *Department of Justice Computer Emergency Response Team*

DOJCERT assists in handling computer security incidents throughout DOJ.<sup>38</sup> DOJ regulations require all components to submit immediate reports summarizing incidents involving the loss of both classified and unclassified systems to DOJCERT.

We contacted DOJCERT officials to determine if the DEA submitted the required incident reports for laptop computers that were identified as lost or stolen during our review period. The DOJ Assistant Director, Property Management Services, told us that DOJCERT was not required to track or report lost and stolen laptops prior to May 2006 when Office of Management Budget Memorandum 06-15, Safeguarding PII was issued. In addition to emphasizing an agency's responsibility to safeguard PII, the memorandum also reminded agencies of the responsibility to promptly report security incidents. According to the DEA, it reported 15 laptops to the Board of Professional Conduct as lost or stolen between May 2006 and June 2007. However, DOJCERT only received reports from the DEA on three laptops during this timeframe.

We discussed this issue with the Unit Chief of the Validation, Integrity, and Penetration Response Unit – the DEA office responsible for reporting lost and stolen laptop incidents to DOJCERT. The Unit Chief told us that if the DEA employee responsible for the lost or stolen laptop does not notify the DEA Help Desk of the incident, then the Validation, Integrity, and Penetration Response Unit would be unaware of the incident and thereby unable to report it to DOJCERT. The Unit Chief said that his office reported all laptop incidents reported to him by DEA personnel.

### **Disposals**

In our 2002 audit report we found that weapons excessed to law enforcement agencies were supported by proper documentation, but the DEA did not follow up with the law enforcement agencies to ensure that shipped weapons were actually received. We recommended that the DEA ensure confirmations for receipt of the weapons were documented by the

---

<sup>38</sup> According to DOJCERT, computer security incidents are any unexpected, unplanned event that could have a negative impact on IT resources. Computer security incidents include the loss of both classified and unclassified systems, unauthorized removal of computer equipment, and exploited weaknesses in a computer system that allows unauthorized access to password files.

Firearms Training Unit. For this follow-up audit, we again tested DEA disposal procedures for its weapons and laptop computers.

Our testing included verifying that DEA records contained proper DEA supporting documentation for destroying and excessing weapons and laptops, including the DEA Forms 12 – Receipt For Cash Or Other Items and the DEA Forms 17 – Firearms Control Record (see Appendices IX and X).<sup>39</sup> We also reviewed documentation on confirmations from law enforcement agencies indicating receipt of DEA surplus weapons. During our follow-up audit, we selected a statistical sample of excessed and destroyed weapons and laptop computers using the data in the DEA's Weapons Database and Fixed Asset Subsystem for the period covering January 1, 2002, through February 28, 2007.

### *Weapons*

According to the DEA Chief Armorer, who is responsible for surplus and destroying DEA weapons, the General Services Administration must provide authorization before a weapon is surplus or destroyed. Weapons that are excessed or destroyed are never deleted from the Weapons Database; instead the weapon category column in the Weapons Database is updated to indicate destroyed or surplus.

Our statistical sample included 295 weapons (43 destroyed and 252 surplus) from a universe of 7,300 destroyed and surplus weapons. We found that the DEA maintained appropriate supporting documentation for all items tested, including completed DEA Forms 17 as appropriate and confirmations from local law enforcement agencies affirming their receipt of the weapons.

### *Laptop Computers*

DEA policy states that disposal documents for laptop computers must be maintained for a period of 3 years after disposal. We selected a sample of excessed and destroyed laptop computers from the DEA's Fixed Asset Subsystem database. Our sample included 166 disposed laptops from a universe of 3,214 destroyed and excessed laptops. Our testing found that the DEA could not provide sufficient supporting documentation for 15 of the

---

<sup>39</sup> The DEA Form 12 – Receipt for Cash or Other Items and the DEA Form 17 – Firearm Control Record are forms used by the DEA to track who has custody of laptop computers and weapons.

166 (9 percent) laptops that it disposed. For 13 of the 15 instances we found that DEA did not retain documentation concerning the disposal for 3 years as required. The DEA provided insufficient documentation to support the disposal for the other two instances.

The DEA's laptop disposal process is decentralized, and the supporting documentation for disposals is maintained at each DEA location worldwide. During our testing, the DEA was unable to provide requested disposal documentation in a reasonable amount of time. We originally asked for supporting documentation for disposals on June 28, 2007. However, it took approximately 90 days to complete our testing. We had to make numerous requests of some field offices to provide supporting disposal documentation or to provide sufficient documentation to allow us to verify the disposal data with the inventory system. Along with our recommendation for the DEA to centralize its laptop inventory records, we also believe the DEA should retain copies of all disposal documentation at centralized locations in each division office to manage the program more effectively, enable quicker reconciliations, and provide adequate audit trails of disposals. This added control would also elevate the DEA's oversight over laptop disposals and increase the overall accountability for excessing laptops.

### **Exit Procedures for Departing Employees**

In our 2002 audit report we found that although there was a category for weapons on the DEA's Employee Clearance Record form, details such as serial numbers or the make and model of DEA weapons assigned to the outgoing employees were not required to be included on the form. In addition, the form did not identify laptop computers as a sign-off item or provide details of the type of accountable property that was retrieved from an employee who left the DEA. We recommended that the DEA ensure that details such as property descriptions, DEA property numbers, and weapon serial numbers were included on the Employee Clearance Records for each employee separating from the agency.

The DEA Form 171a – Employee Clearance Record (see Appendix XII), is used by the DEA to document that departing personnel have returned DEA property assigned to the individual. Items such as building passes, laptops, credentials, and weapons are included on the form. The DEA requires that an Employee Clearance Record certifying that all DEA-issued property has been returned to the DEA be completed for all departing employees. The "Security Activity" section of the form addresses weapons and the "Immediate Supervisor" section addresses personal custody property items, which includes assigned laptops. The separating employee must obtain

signatures of responsible officials (e.g., Primary Firearms Instructors and Property Custodial Assistants) on the Employee Clearance Record verifying that all DEA-issued weapons and laptops were turned over to the DEA before employment separation.

During our follow-up audit we reviewed Employee Clearance Records at the selected DEA field division offices. We reviewed Employee Clearance Records for departing employees for the period of January 1, 2005, through August 2, 2007. We tested the forms to verify that for weapons the make, model, caliber, and serial number was included, and the appropriate official signed the form verifying receipt of the DEA-issued weapon. Our testing found that the DEA was appropriately completing this section on the Employee Clearance Record forms, providing the DEA a sound control over the weapons assigned to departing employees.

Our review of the Employee Clearance Record forms found that appropriate DEA supervisors signed the form certifying that all personal property items had been returned by the separating employee. However, the DEA was still not documenting the Employee Clearance Records with specifics on returned laptops, particularly DEA property numbers and laptop make and model plus its serial numbers. Therefore, due to the lack of specific details used in identifying a laptop computer on the Employee Clearance Records, we were unable to determine whether the outgoing employee returned the specific DEA-issued laptop.

In 2002 the DEA revised its policy to strengthen its procedures for ensuring that departing employees return all property that was issued to them or reimburse the government for the cost of the property if it was not returned. Our review concluded that the DEA's employee exit controls for weapons were adequate, and the DEA was complying with the associated procedures. However, our testing of Employee Clearance Records revealed that the DEA procedures to account for the proper return of DEA-issued laptops were inadequate, thereby increasing the potential for property loss upon employee separation.

## **Conclusion**

During this follow-up audit we found that the DEA has improved its internal controls over its weapons and laptop computers in some areas, such as in conducting annual physical inventories. However, our audit revealed that other deficiencies in the DEA's control over its weapons and laptop computers continued since our previous audit. Specifically, the DEA failed to adequately maintain documentation for laptop disposals, neglected to submit

required semiannual reports of weapon and laptop losses to DOJ, and did not institute adequate procedures to ensure that property is recovered from employees before they leave DEA service.

## **Recommendations**

We recommend that the DEA:

5. Ensure that each division office maintains supporting documentation for laptop purchases and disposals.
6. Prepare and submit to DOJ Justice Management Division complete and accurate semiannual Department Theft Reports regarding the loss of weapons and laptop computers and to DOJCERT incident reports regarding the loss of laptop computers.
7. Strengthen the exit processing for departing employees to ensure that documentation on the Employee Clearance Record clearly indicates specifics on remitted laptops.

## STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

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

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

Our audit identified several areas where the DEA was not in compliance with the laws and regulations referred to above. Specifically, we determined that the DEA did not always report its lost and stolen weapons and laptops to DOJ as required. Additionally, we found that the DEA did not notify DOJCERT of all laptops lost or stolen. With respect to transactions that were not tested, nothing came to our attention that caused us to believe that DEA management was not in compliance with the laws and regulations cited above.

## OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted this follow-up audit of the DEA's control over weapons and laptop computers. The purpose of the follow-up audit was to assess whether adequate corrective action had been taken on findings and 22 recommendations in the August 2002 audit report. Those recommendations stated that the DEA should:

- (1) reiterate to all DEA employees the guidelines for the security, safety, and storage of weapons as outlined in the DEA firearms policy;
- (2) reiterate to all DEA employees the policy for reporting losses of DEA property as outlined in the DEA firearms policy;
- (3) provide semiannual Department Theft Reports for the reporting periods from July 1 to December 31, 1999, and January 1 to December 31, 2000;
- (4) ensure the timely and complete submission of future semiannual Department theft reports;
- (5) ensure that the lost, missing, or stolen weapons are promptly entered into the NCIC;
- (6) ensure that appropriate action is taken on laptop computers that are subsequently determined to be lost, stolen, or missing as a result of the reconciliation of the property inventory;
- (7) ensure that a perpetual list of lost, stolen, or missing laptop computers is maintained and that notifications and investigative procedures are performed;
- (8) develop internal controls, operating manuals, audit trails, and system requirements appropriate to ensure the reliability of inventory data in the weapons database;
- (9) ensure that a valid inventory is available to all Property Custodial Assistants based on the completed reconciliation of the Fixed Asset Subsystem inventory records to correct the problems created from the conversion the old M-204 system;

- (10) integrate the DEA's financial system with the property management systems so that the inventory is routinely updated in a timely manner when a weapon or laptop computer is purchased;
- (11) ensure that all purchases are entered in a timely manner into the Fixed Asset Subsystem inventory;
- (12) ensure that employees who receive shipments of weapons do not have access to the weapons database;
- (13) record in the Fixed Asset Subsystem the names of the individuals who are accountable for laptop computers instead of the Property Custodial Assistants;
- (14) ensure Property Custodial Assistants maintain adequate property records to show current assignment of laptop computers;
- (15) ensure that field division level Property Custodial Assistants are advised in a timely manner by DEA headquarters of purchases and transfers of property items that pertain to their division;
- (16) ensure that hand receipts for transfers are used throughout the DEA;
- (17) ensure that details such as property descriptions, DEA property numbers, and weapon serial numbers are included on Employee Clearance Records;
- (18) ensure that updates to the property system are made in a timely manner;
- (19) ensure that the physical inventory of weapons is performed annually as required by DEA headquarters;
- (20) segregate the duties of staff who take physical inventories, perform reconciliations, and modify the property management system;



- (21) ensure that inventories are validated as required for each unit within DEA headquarters; and
- (22) ensure that confirmations from law enforcement entities are received and forwarded to the Firearms Training Unit when weapons are excessed.

Overall, the DEA agreed with these recommendations and stated that it had taken steps to address them. As of April 20, 2005, all recommendations had been closed.

We performed the follow-up audit in accordance with the *Government Auditing Standards* and included such tests of the records and procedures that we considered necessary. Our testing covered the period between January 1, 2002, and June 30, 2007.

We obtained an understanding of the control environment for weapons from DEA management at the Firearms Training Unit located in Quantico, Virginia, which is responsible for the overall management of the weapon property system for all DEA weapons. We obtained an understanding of the control environment for DEA laptop computers from the Property Management Unit located at DEA headquarters. We performed on-site audit work between May 2007 and July 2007 at DEA headquarters' offices and the Firearms Training Unit. We conducted on-site audit work between July 2007 and August 2007 at the DEA field division offices in Chicago, Illinois; Denver, Colorado; Houston, Texas; Los Angeles, California; Miami, Florida; and New York, New York.

To examine the DEA's efforts to identify lost and stolen weapons and laptop computers, we obtained a list of all such losses that occurred since January 1, 2002, and reviewed the available files and the circumstances surrounding those losses. We also obtained DOJ Semiannual Reports of lost or stolen property that were submitted to the DOJ Security Officer. For lost or stolen weapons, we queried NCIC to determine if information on the lost property was entered in the NCIC database.

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 January 1, 2002); and (5) physically inspected property. We tested internal controls pertaining to weapons and laptop computers in the following areas:

- purchasing and recording in the official property database (the Fixed Asset Subsystem for laptops and the Weapons Database for firearms),
- the return of items from separated employees,
- physical inventories, including separation of duties, and
- disposals, including signed receipts for surplus weapons.

We tested these controls through a sample from the DEA's 14,449 weapons and 7,381 laptop computers reported in the corresponding inventory records as of April 2007. In total, we reviewed 7,306 items, including 4,299 weapons and 3,007 laptop computers. Details about the universe from which these samples were taken and about the samples themselves may be found in Appendix VIII. Our tests also included the following:

- Samples of weapon and laptop computer purchases, as recorded in purchase documents, to ensure that the items were recorded in the Fixed Asset Subsystem and the Weapons Database.
- 100 percent testing of stock weapons maintained at the Firearms Training Unit, and weapons assigned to Special Agents at DEA headquarters' offices to ensure the item was accurately recorded in the Weapons Database.
- 100 percent testing of laptop computers located at DEA headquarters' offices to ensure the laptop computers were accurately recorded in the Fixed Asset Subsystem.
- Testing of personally owned weapons authorized to be carried for official use by Special Agents included in our testing conducted at DEA headquarters' offices and at the field sites where we conducted our sample testing.

We also reviewed the documentation at field site locations where we conducted our sample testing to determine if all weapons and laptop computers were returned. Moreover, we reviewed disposal actions initiated between January 1, 2002, and February 28, 2007, to ensure these actions were adequately supported.

## ABBREVIATIONS AND FORMS

### Abbreviations:

DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Response Team
FBI	Federal Bureau of Investigation
NCIC	National Crime Information Center
OIG	Office of the Inspector General
PII	Personally Identifiable Information
POV	Privately Owned Vehicle
SEPS	Security and Emergency Planning Staff

### Forms:

DEA-12	Receipt for Cash or Other Items
DEA-17	Firearms Control Record
DEA-29	Personal Property Negligence/Liability Assessment
DEA-171a	Employee Clearance Record
DEA-609	Request for Authority to Carry a Personally Owned Firearm

This page intentionally left blank.

## CIRCUMSTANCES AND ACTIONS TAKEN FOR LOST AND STOLEN WEAPONS

Item Number	DEA Form 29 Report Date	Description of Incident	Action Taken
1	11/1/2001	Weapon determined missing during inventory.	Clearance
2	9/6/2001	Weapon reported destroyed in Bombing and fire in 1990.	Clearance
3	1/18/2002	Weapon stolen from Special Agent.	Clearance
4	4/19/2002	Weapon determined unaccounted for during inventory - Assigned to deceased agent. Action taken to remove weapon from inventory in March 2002.	Clearance
5	5/29/2002	Weapon stolen from Special Agent's privately owned vehicle parked at a school.	Suspended 1 day
6	5/30/2002	Weapon stolen -- left weapon on boat loading dock area - walked away - came back later and weapon was gone.	Suspended 1 day
7	6/12/2002	Weapon stolen from an official government vehicle parked at restaurant while Special Agent had lunch. Special Agent transferred to another agency before action taken.	Administratively closed
8	10/17/2002	Weapon stolen from official government vehicle while agent was exercising at public facility.	Suspended 3 days
9	7/31/2002	Weapon stolen from unattended official government vehicle parked at hotel.	Suspended 1 day and paid \$516.63
10	11/20/2002	Weapon stolen from official government vehicle at autobody shop; Special Agent left weapon in range bag in the car.	Suspended 1 day and paid \$471.00
11	12/9/2002	Weapon stolen from privately owned vehicle parked at shopping center.	Suspended 3 days
12	11/22/2002	Weapon stolen from official government vehicle parked at residence.	Suspended 1 day
13	12/10/2002	Weapon left at range or removed from official government vehicle-unknown.	Suspended 2 days and paid \$210.00
14	10/20/2002	Weapon stolen from privately owned vehicle while Special Agent was in Canada.	Suspended 3 days
15	1/13/2003	Weapon stolen from privately owned vehicle while at restaurant.	Suspended 1 day and paid \$532.13
16	3/3/2003	Weapon stolen from official government vehicle that was burglarized.	Suspended 1 day
17	3/3/2003	Weapon stolen from official government vehicle that was burglarized.	Suspended 1 day

<b>Item Number</b>	<b>DEA Form 29 Report Date</b>	<b>Description of Incident</b>	<b>Action Taken</b>
18	2/27/2003	Weapon stolen from official government vehicle while at gym.	Suspended 3 days
19	3/4/2003	Weapon stolen from privately owned vehicle while Special Agent was shopping.	Suspended 3 days
20	5/7/2003	Weapon lost transferring between official government vehicle and privately owned vehicle.	Suspended 1 day
21	4/30/2003	Weapon lost out of motorcycle day pack during day trip.	Suspended 1 day
22	2/6/2003	Weapon stolen from official government vehicle parked at residence.	Suspended 4 days
23	9/22/2003	Weapon stolen from briefcase in residence.	Clearance
24	11/3/2003	Weapon & official government vehicle destroyed in a wildfire.	Clearance
25	1/26/2004	Weapon was missing a part when Special Agent reported for military duty.	Letter of Caution
26	5/20/2004	Weapon stolen from Special Agent's locked residence which had burglar alarm.	Clearance
27	2/26/2004	Weapon stolen from residence - forced entry.	Clearance
28	4/30/2004	Weapon stolen from residence in Lima, Peru.	Clearance
29	9/9/2004	Weapon stolen from official government vehicle parked at restaurant.	Suspended 3 days
30	7/21/2003	Weapon stolen from official government vehicle parked at a summer rental house.	Suspended 5 days
31	9/1/2004	Weapon lost – unable to determine when and where.	Suspended 30 days
32	9/2/2004	Weapon lost – Special Agent lost backpack and was unable to determine where.	Suspended 1 day and paid \$237.82
33	10/12/2004	Weapon lost – Special Agent/Primary Firearms Instructor failed to follow up after sending for repair.	Letter of Caution
34	10/19/2004	Weapon stolen from privately owned vehicle parked at friend's residence.	Suspended 3 days and paid \$185.95
35	1/10/2003	Weapon lost – Special Agent/Primary Firearms Instructor failed to put weapon into office inventory.	Letter of Reprimand
36	10/12/2004	Weapon stolen from official government vehicle parked at residence.	Suspended 4 days
37	10/12/2004	Weapon stolen from official government vehicle parked at residence.	Suspended 4 days
38	10/14/2004	Weapon stolen from official government vehicle parked at restaurant.	Suspended 3 days

<b>Item Number</b>	<b>DEA Form 29 Report Date</b>	<b>Description of Incident</b>	<b>Action Taken</b>
39	11/22/2004	Weapon stolen from official government vehicle parked at convenience store while Special Agent was buying coffee.	Suspended 2 days and paid \$292.22
40	11/15/2004	Weapon stolen – Special Agent left weapon in official government vehicle that was burglarized.	Suspended 4 days and paid \$953.60
41	11/15/2004	Weapon stolen – Special Agent left weapon in official government vehicle that was burglarized.	Suspended 4 days and paid \$953.60
42	2/7/2005	Weapon stolen – Special Agent left weapon in official government vehicle that was burglarized.	Suspended 2 days and paid \$138.12
43	1/4/2005	Weapon stolen – Special Agent left weapon in privately owned vehicle that was burglarized.	Suspended for 3 days
44	2/18/2005	Weapons stolen – inactivated weapons used as part of the DEA's road museum.	Clearance
45	2/18/2005	Weapons stolen – inactivated weapons used as part of the DEA's road museum.	Clearance
46	2/18/2005	Weapons stolen – inactivated weapons used as part of the DEA's road museum.	Clearance
47	3/16/2005	Weapon stolen from residence in Puerto Rico.	Clearance
48	3/16/2005	Weapon stolen from residence in Puerto Rico.	Clearance
49	4/18/2004	Weapon stolen from official government vehicle parked in front of residence.	Suspended 3 days and paid \$151.55
50	7/1/2005	Weapon lost - not sure where or how loss occurred; may have fallen into trash basket at work.	Letter of Reprimand
51	8/23/2005	Weapon stolen apparently by moving company employees.	Clearance
52	8/23/2005	Weapon stolen apparently by moving company employees.	Clearance
53	10/5/2005	Weapon lost – Special Agent left weapon on roof of car and drove off.	Letter of Reprimand
54	11/25/2005	Weapon that cannot fire live ammunition lost – determined missing during inventory.	Clearance
55	11/28/2005	Weapon stolen – Special Agent left firearm in his official government vehicle which was burglarized.	Suspended 3 days
56	10/18/2005	Weapon stolen – Special Agent put weapon in purse while at social function at bar in Jamaica.	Suspended 3 days
57	1/4/2006	Weapons stolen – Special Agent /Primary Firearms Instructor had weapons in official government vehicle parked in residence driveway.	Suspended 7 days
58	1/4/2006	Weapons stolen – Special Agent /Primary Firearms Instructor had weapons in official government vehicle parked in residence driveway.	Suspended 7 days

<b>Item Number</b>	<b>DEA Form 29 Report Date</b>	<b>Description of Incident</b>	<b>Action Taken</b>
59	3/29/2006	Weapon stolen – Special Agent placed in a briefcase and left behind in a restaurant.	Suspended 1 day
60	3/16/2006	Weapon stolen out of Special Agent's office. It was believed that a carpet installer stole it.	Clearance
61	12/13/2005	Weapons (shotguns) stolen out of official government vehicle.	Suspended 4 days
62	12/13/2005	Weapons (shotguns) stolen out of official government vehicle.	Suspended 4 days
63	6/29/2006	Weapon stolen when parents' home was burglarized.	Clearance
64	7/18/2006	Weapon stolen – Special Agent's residence burglarized.	Clearance
65	4/12/2006	Weapon stolen – Special Agent assigned to Bogota left firearm in his official government vehicle to go inside a school building and his vehicle was burglarized during the 50 minutes he was inside.	Suspended 5 days
66	4/16/2006	Weapon stolen when Assistant Special Agent in Charge left firearm in his official government vehicle which was broken into and his personal firearm was stolen.	Suspended 5 days
67	10/13/2006	Weapon stolen from official government vehicle parked at middle school while Special Agent watched a football game.	Suspended 7 days
68	11/17/2003	Weapon stolen from official government vehicle parked in restaurant parking lot.	Suspended 5 days and paid \$474.93
69	9/8/2006	Weapon stolen – Special Agent left firearm in official government vehicle while getting lunch and vehicle was burglarized.	Suspended 7 days
70	2/5/2007	Weapon stolen – Special Agent put firearm in glove box because nightclub was searching patrons and he didn't want to give away that he was law enforcement.	Administratively Closed
71	9/5/2006	Weapon stolen when residence was burglarized.	Clearance
72	5/8/2007	Weapon stolen when residence was burglarized.	Clearance
73	4/5/2007	Weapon stolen when residence was burglarized.	Clearance
74	11/28/2001	Weapon lost in transit to receive for repairs.	Clearance
75	7/12/2002	Weapon lost – Special Agent left weapon at police firing range.	Letter of Caution
76	7/29/2002	Weapon stolen from official government vehicle parked at residence in driveway.	Suspended 1 day
77	7/29/2002	Weapon stolen from official government vehicle parked in residence driveway.	Suspended 1 day



<b>Item Number</b>	<b>DEA Form 29 Report Date</b>	<b>Description of Incident</b>	<b>Action Taken</b>
78	11/22/2002	Weapon stolen when Special Agent left the weapon in an official government vehicle for 3 days.	Letter of Caution
79	6/4/2003	Weapon stolen from official government vehicle parked at residence.	Suspended 3 days
80	11/21/2002	Weapon stolen from hotel room - Special Agent out on balcony.	Clearance
81	10/14/2003	Weapon stolen from police vehicle while Special Agent had lunch.	Suspended 1 day
82	1/16/2004	Weapon stolen from locked bedroom at residence.	Clearance
83	8/18/2003	Weapon stolen from official government vehicle while watching son at football practice.	Suspended 4 days
84	12/17/2004	Weapon stolen from official government vehicle parked at residence.	Suspended 5 days
85	9/20/2005	Weapon stolen from privately owned vehicle parked in residence driveway.	Suspended 3 days
86	1/25/2006	Weapon stolen by Special Agent's son.	Clearance
87	10/18/2005	Weapon lost – Special Agent left weapon on airplane.	Suspended 7 days
88	12/12/2005	Weapon lost – Special Agent left weapon on airplane.	Suspended 3 days
89	12/4/2005	Weapon lost – Special Agent left weapon in airport restroom.	Letter of Caution
90	4/25/2006	Weapon lost – Special Agent left weapon in supermarket.	Suspended 5 days
91	4/6/2007	Weapon lost or unaccounted for – during Hurricane Katrina response on August 30, 2005, multiple weapons were provided to commissioned local law enforcement officers and documentation was not always obtained.	Clearance

Source: OIG analysis of DEA Board of Professional Conduct case files

This page intentionally left blank.

**CIRCUMSTANCES AND ACTIONS TAKEN  
FOR LOST AND STOLEN LAPTOPS<sup>40</sup>**  
BOARD OF PROFESSIONAL CONDUCT CASES OPENED  
JANUARY 1, 2002 THROUGH JUNE 30, 2007

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
1	1/2/2002	Laptop sent to Information Systems for disposal without proper documents. Whereabouts unknown.	Unable to Determine	Clearance
	1/2/2002	Laptop sent to Information Systems for disposal without proper documents. Whereabouts unknown.	Unable to Determine	Clearance
	1/2/2002	Laptop sent to Information Systems for disposal without proper documents. Whereabouts unknown.	Unable to Determine	Clearance
2	1/4/2002	Laptop was replaced on 6/17/98 and no documentation could be found to show the exchange. Laptop most likely disposed of.	Unable to Determine	Clearance
3	9/6/2001	Laptop cannot be located during inventory and investigation and search were negative.	Unable to Determine	Clearance
4	1/14/2002	Missing laptop since May 1998.	Unable to Determine	Clearance
5	10/30/2001	Laptop was returned to Computer Specialist and custody was not maintained. Whereabouts unknown.	Unable to Determine	Clearance
6	1/17/2002	Laptop not found during inventory. Investigation was negative. Laptop believed to be surplus and disposed.	Unable to Determine	Clearance
7	11/14/2001	Laptop not found during inventory and no records are available to show its whereabouts.	Unable to Determine	Clearance
8	10/29/2001	Laptop not found during inventory and no records exist to account for it. Laptop considered obsolete.	Unable to Determine	Clearance
9	2/5/2002	Laptop not found during inventory and no records exist to account for it. Laptop considered obsolete.	Unable to Determine	Clearance
10	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance

<sup>40</sup> As previously reported, DEA did not begin encrypting laptops until November 2006. Therefore, it is unlikely that any laptop lost before this date was encrypted.

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
10 (continued)	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
	10/29/2001	Investigation determined these laptops were used for parts and the remainder were burned during a scheduled DEA burn in Modesto, CA.	Unable to Determine	Clearance
11	8/10/2001	Laptop was turned in for destruction and stored in a secure facility. DEA personnel disposed of obsolete equipment but proper documentation was not completed so whereabouts of laptop is unknown. Assumed destroyed.	Unable to Determine	Clearance
12	2/5/2002	Found missing during routine inventory in 1998.	Unable to Determine	Clearance
13	UTD	Special Agent accidentally packed the laptop with household goods before move. Laptop was missing when household goods were delivered to new location.	Unable to Determine	Letter of Reprimand
14	4/8/2002	Discovered during inventory.	Unable to Determine	Letter of Counseling
15	5/13/2002	A shared laptop was not found during an inventory check. An investigation was undertaken with negative results. Laptop was obsolete at the time of the inventory.	Unable to Determine	Letter of Counseling

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
16	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
	5/9/2002	Laptops reflected on SAOP's inventory but unable to locate at the Office of Resource Management. Laptops are obsolete and assumed destroyed.	Unable to Determine	Clearance
17	8/28/2002	Laptop determined missing during inventory but was not removed from the listing until 8/02.	Unable to Determine	Clearance
18	UTD	Laptop disposed in 1994 but not removed from inventory.	Unable to Determine	Clearance
19	5/6/2002	Laptop was replaced by UNYSIS but the DEA # was not transferred to replacement computer.	Unable to Determine	Clearance
20	6/5/2002	Laptop was stolen when agent left it unattended at hotel pool.	Unable to Determine	Letter of Reprimand - Financial Liability - \$1,050

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
21	8/30/2002	Laptop sent to Information Systems for repairs. Repair was not warranted and item was surplused without proper records and cannot be found during inventory.	Unable to Determine	Clearance
22	9/3/2002	Telecommunications Specialist left laptop in official government vehicle in front of residence overnight. Rear window broken, laptop stolen.	Unable to Determine	Letter of Reprimand - Financial Liability - \$499
23	5/16/2002	Could not locate during routine inventory - believed to have been replaced with another laptop that was disposed of.	Unable to Determine	Clearance
24	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
	10/31/2002	Items reported missing at inventory.	Unable to Determine	Clearance
25	10/28/2002	Unable to locate during routine inventory.	Unable to Determine	Clearance
	10/28/2002	Unable to locate during routine inventory.	Unable to Determine	Clearance
26	10/1/2002	Temporary quarters in St. Maarten burglarized.	Unable to Determine	Clearance
27	10/28/2002	Could not locate during routine inventory - records indicate destroyed in March 2000 but lacking proper documentation.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
28	11/6/2002	Amendment to previous report, instead of DEA 193841 the # 193842 should be reported.	Unable to Determine	Clearance
29	10/2/2002	Could not locate during inventory and transfer to new storage facility.	Unable to Determine	Clearance
30	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
	9/27/2002	Could not locate during routine inventory - three of responsible retired.	Unable to Determine	Clearance
31	8/14/2001	Item noted as missing in February 2000, DEA FORM 29 Reported 8/14/01, Investigator signed 12/2/2002.	Unable to Determine	Clearance
32	10/3/2002	Laptop left at Gateway Center Security checkpoint. Laptop was not recovered.	Unable to Determine	Letter of Counseling
33	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
33 (continued)	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
	11/7/2002	Laptop discovered missing during inventory and later found to be surplus, awaiting destruction, or was absent from the 1998 inventory.	Unable to Determine	Clearance
34	11/22/2002	Special Agent left laptop in taxi in Bangkok, contained no sensitive or classified information. Laptop was not recovered.	Did not contain sensitive or classified information	Letter of Counseling
35	10/9/2002	Inventory February 2002 showed laptop, it was noted as missing July 2002, responsible person is no longer a DEA employee.	Unable to Determine	Clearance
36	11/12/2002	Government leased quarters burglarized.	Unable to Determine	Clearance
37	11/19/2002	Loaned to Mexican counterparts and never returned.	Unable to Determine	Clearance
38	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance



Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
38 (continued)	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
	11/21/2002	Items reported missing at inventory / Item destroyed.	Unable to Determine	Clearance
39	UTD	Could not locate during routine inventory - File states DEA-29 was completed, but it was not in the file. - Agent had retired.	Unable to Determine	Clearance
40	1/9/2003	Assigned to group-no one person totally responsible-inventory showed missing - last seen 1994.	Unable to Determine	Clearance
41	10/18/2002	An old laptop could not be accounted for during inventory, a search of office did not locate property.	Unable to Determine	Clearance
42	12/18/2002	During routine annual inventory laptop was noted as missing.	Unable to Determine	Clearance
43	1/17/2003	Laptop discovered missing during inventory.	Unable to Determine	Clearance
	1/17/2003	Laptop discovered missing during inventory.	Unable to Determine	Clearance
44	3/3/2003	Laptop missing after offsite Task Force Office was burglarized.	Unable to Determine	Clearance
45	1/28/2003	Laptop disappeared, possibly collected with garbage.	Unable to Determine	Clearance
46	4/16/2003	Special Agent left laptop in official government vehicle while in physical fitness center and it was stolen out of the vehicle. No sensitive or classified information.	Did not contain sensitive or classified information	Letter of Counseling
47	5/12/2003	Laptop inadvertently left off previous reports concerning missing laptops.	Unable to Determine	Clearance
48	4/10/2003	Stolen from a secured work space - FDLE Task Force while Special Agent on a 45 day TDY. Per DEA-6 laptop did not contain any classified or sensitive data. Item discovered stolen during a routine inventory.	Did not contain sensitive or classified information	Letter of Counseling
49	11/15/2002	The wrong DEA tracking number was placed on the laptop, a DEA FORM 29 was filed, they noted the error and documented the situation. The laptop was never missing.	Unable to Determine	Clearance
50	2/4/2003	Item was erroneously reported as missing, but was found to be appropriately accounted for (returned to DOJ CATS).	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
51	5/11/2003	Telecommunications Specialist left laptop in his garage and it was stolen. According to him it contained sensitive case information.	Contained sensitive information	Letter of Reprimand
52	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
	6/24/2003	Laptops discovered missing after physical inventory in 2002.	Unable to Determine	Clearance
53	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
53 (continued)	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
	10/30/2003	Laptops discovered missing after physical inventory in 2003.	Unable to Determine	Clearance
54	11/3/2003	Special Agent transferred from duty station and left laptop for use by other Special Agents. During the annual inventory the laptop could not be accounted for.	Unable to Determine	Letter of Counseling
55	11/4/2003	Laptop transferred between multiple employees. However, all 3 employees are retired and supporting documents believe to be destroyed.	Unable to Determine	Clearance
56	11/1/2003	Could not locate during routine inventory-probably disposed of in 1998.	Unable to Determine	Clearance
57	10/23/2003	Could not locate during routine inventory-sent to Dallas warehouse for disposal-no paperwork found-laptop purchased in 1992 so only had scrap value.	Unable to Determine	Clearance
58	12/10/2003	Could not locate during routine inventory - probably lost during several exchanges between several Intelligence Division personnel.	Unable to Determine	Clearance
59	10/8/2003	Investigation indicates the laptop was most probably loaned to the Mexico SIU. Unable to determine responsibility.	Unable to Determine	Clearance
60	10/17/2003	Could not locate during inventory in 10/2003-last shown on inventory in July 2001.	Unable to Determine	Clearance
61	2/11/2004	Stolen from official government vehicle.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
62	11/21/2003	Could not locate during inventory in 12/2003.	Unable to Determine	Clearance
	11/21/2003	Could not locate during inventory in 12/2003.	Unable to Determine	Clearance
	11/21/2003	Could not locate during inventory in 12/2003.	Unable to Determine	Clearance
	11/21/2003	Could not locate during inventory in 12/2003.	Unable to Determine	Clearance
63	10/31/2003	Stolen from secure hotel area, investigation indicates a hotel employee was involved. Office of Congressional and Public Affairs was using the DEA computer for a presentation.	Unable to Determine	Clearance
64	2/25/2004	Laptop left unattended at reception and was stolen.	Unable to Determine	Letter of Reprimand - Financial Liability - \$699.77
65	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
65 (continued)	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
	10/27/2003	Laptop discovered lost during inventory 9/15/03. Later discovered laptops were cannibalized for components by former contract employee.	Unable to Determine	Clearance
66	4/22/2004	During the annual inventory FY2003 the laptop computer was unaccounted for. During the investigation it was noted that the previous office in Pakistan was closed and the laptop was stored with other items in another location.	Unable to Determine	Clearance
67	3/31/2004	Could not locate during inventory in 2003 - Mexico City.	Unable to Determine	Clearance
68	10/12/2002	Could not locate on inventory in Aug. 2001.	Unable to Determine	Clearance
69	4/15/2004	Could not locate on inventory in Nov. 2003. Believed to have been sent to Mexico City for repairs and stolen from there.	Unable to Determine	Clearance
70	4/13/2004	Laptop stolen from locked hotel room while agent was on vacation in Florida.	Unable to Determine	Clearance
71	11/18/2003	In 2002 laptops transferred to LA Field Division for repair. Determined too costly to repair so both placed in surplus status. Could not locate in inventory in Oct. 2003.	Unable to Determine	Clearance
	11/18/2003	In 2002 laptops transferred to LA Field Division for repair. Determined too costly to repair so both placed in surplus status. Could not locate in inventory in Oct. 2003.	Unable to Determine	Clearance
72	6/4/2004	Agent thinks laptop was stolen from official government vehicle while agent lunched at local restaurant on 4/19/04. However, agent also utilized a full service car wash on 4/16/04. Agent didn't discover until 4/21/04.	Unable to Determine	Letter of Reprimand - Financial Liability - \$1,990.58
73	6/3/2004	Laptop stolen from checked luggage on return trip from Botswana.	Unable to Determine	Clearance
74	6/18/2004	Laptop noted as missing during the annual inventory, investigation indicates the computer was returned to HQ but no documentation was found and computer could not be located.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
75	6/25/2004	The investigation shows that the exact date the laptop was missing is unknown. Used the DEA FORM 29 date. No sensitive or classified information on laptop.	Did not contain sensitive or classified information	Letter of Counseling
76	6/21/2004	Special Agent transferred from one duty station to another and apparently left laptop at previous duty station since it belonged to that group. Later contacted regarding location of laptop, it could not be found. Laptop was ultimately located.	Unable to Determine	Clearance
77	7/16/2004	Stolen from Dominican National Directorate, Command and Control Center a joint facility in Santo Domingo.	Unable to Determine	Clearance
78	9/9/2004	Stolen from official government vehicle parked at restaurant while Special Agent on TDY - NCIC 29503.	Unable to Determine	Suspension - 3 days
79	7/2/2004	Laptop used by Foreign Operations Group and not returned. Unknown Last DEA Agent to use laptop and no records to locate.	Unable to Determine	Clearance
80	10/6/2004	Special Agent left laptop in taxi cab trunk and it was stolen.	Unable to Determine	Letter of Counseling
81	10/26/2004	Stolen from hotel room.	Unable to Determine	Clearance
82	10/7/2004	Laptop reported missing but was found behind metal shelving unit in equipment storage area on 7/28/05.	Unable to Determine	Letter of Counseling
83	11/2/2004	Laptop discovered missing during inventory in Oct 2004. Laptop subsequently found.	Unable to Determine	Clearance
84	7/12/2004	Laptop stolen from official government vehicle	Unable to Determine	Suspension - 2 days - Financial Liability - \$416.47
85	11/16/2004	Laptop discovered lost during inventory in Nov 2004.	Unable to Determine	Clearance
86	6/30/2005	Stolen from official vehicle	Unable to Determine	Clearance
87	6/30/2005	Laptop left in locked official government vehicle, vehicle broken into and laptop stolen, nothing in file indicated the classification of information on the laptop.	Unable to Determine	Letter of Reprimand
88	7/5/2005	Support staff member believes he left in official government vehicle but search came up with nothing.	Unable to Determine	Letter of Reprimand
89	8/20/2005	Could not locate during 2004 inventory.	Unable to Determine	Clearance

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
90	11/16/2005	Laptop stolen from official government vehicle at 3:00 a.m. while agent was on duty but away from vehicle.	Unable to Determine	Letter of Counseling
91	12/15/2005	Laptop stolen from wire room cubicle	Unable to Determine	Clearance
92	7/5/2005	Laptop discovered missing during inventory. Laptop has been destroyed or surplus.	Unable to Determine	Clearance
	7/5/2005	Laptop discovered missing during inventory. Laptop has been destroyed or surplus.	Unable to Determine	Clearance
93	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
	10/10/2005	Laptops discovered missing during inventory in July 2005. Three laptops subsequently found. Laptops with DEA #s 317287; 317284; and 343308 were still missing as of 3/13/06 (date of last DEA-29).	Unable to Determine	Clearance
94	3/9/2006	Special Agent inadvertently left bag outside vehicle when loading luggage after a flight.	Unable to Determine	Letter of Counseling
95	4/12/2006	Special Agent loaned laptop to Aruban Police Dept. without obtaining a receipt in 2002. Believe Aruban Police destroyed when updating T-III Room.	Unable to Determine	Letter of Counseling

Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
96	4/21/2005	Special Agent lost laptop approx. Aug 04 but not reported. Found missing during inventories in November 2004 and April 2005. Agent told to look for it after 2004 inventory but the then supervisor retired and nothing was done until after 2005 inventory. Agent failed to file DEA-29.	Unable to Determine	Letter of Reprimand - Financial Liability - \$340.36
97	8/5/2005	Laptop was used by an intelligence analyst, he turned it in when he transferred, when the unit got a new property custodian and she conducted the inventory the laptop was noted as unaccounted for.	Unable to Determine	Clearance
98	7/14/2006	Laptop discovered missing during inventory in June 2005.	Unable to Determine	Clearance
99	8/17/2006	TFO signed out laptop on March 14, 2005 but has not idea where it is now.	Unable to Determine	Clearance
100	8/7/2006	Laptop was 15 years old and no present Paris CO employees were ever assigned it.	Unable to Determine	Clearance
101	7/14/2006	Loaned to Aruban Police in 2002. Aruban Police think they were returned in 2005.	Unable to Determine	Clearance
	7/14/2006	Loaned to Aruban Police in 2002. Aruban Police think they were returned in 2005.	Unable to Determine	Clearance
102	7/20/2006	May 2004 was the last time the Special Agent recalls having the laptop. It was determined to be old and outdated and obsolete left at previous field office.	Unable to Determine	Clearance
103	8/4/2006	Laptop discovered missing during inventory in July 2006.	Unable to Determine	Clearance
104	9/1/2006	Laptop discovered missing during inventory.	Unable to Determine	Clearance
105	7/24/2006	Laptop discovered missing during inventory.	Unable to Determine	Clearance
	7/24/2006	Laptop discovered missing during inventory.	Unable to Determine	Clearance
106	11/27/2006	Laptop stolen from privately owned vehicle while on leave in Phoenix.	Unable to Determine	Letter of Reprimand - Financial Liability - \$1,800.63
107	11/29/2006	Discovered thru routine inventory in Nov. 06.	Unable to Determine	Clearance
108	12/1/2006	Agent stated surplus in May or June 2005. Said DEA-29 was done but paperwork not found.	Unable to Determine	Clearance
109	2/6/2007	Inventory July 2005 shows laptop unaccounted for. DEA FORM 29 filed in February 2007. Special Agent to whom laptop assigned states it was returned to (IT) for repair long ago.	Unable to Determine	Letter of Counseling



Item Number	DEA Form 29 Report Date	Description of Incident	Contents of Laptop	Action Taken
110	11/14/2006	Laptop computer apparently transferred to multiple locations and an employee who was fired for other issues was involved with this laptop. Result laptop can't be located.	Unable to Determine	Clearance

Source: OIG analysis of the DEA Board of Professional Conduct case files

This page intentionally left blank.

## ANALYSIS OF LOST AND STOLEN DEA WEAPONS

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
1	Lost	410	NO	NO
2	Lost	4207	NO	NO
3	Stolen	96	NO	NO
4	Lost	0	YES	NO
5	Stolen	6	NO	YES
6	Stolen	13	NO	YES
7	Stolen	1	YES	YES
8	Stolen	13	NO	YES
9	Stolen	1	YES	YES
10	Stolen	26	NO	NO
11	Stolen	78	NO	YES
12	Stolen	25	NO	YES
13	Lost	15	NO	YES
14	Stolen	1	YES	YES
15	Stolen	3	YES	YES
16	Stolen	2	YES	UTD <sup>41</sup>
17	Stolen	2	YES	UTD
18	Stolen	2	YES	YES
19	Stolen	3	YES	YES
20	Lost	5	NO	YES
21	Lost	20	NO	YES
22	Stolen	20	NO	YES
23	Stolen	8	NO	YES
24	Lost	8	NO	NO
25	Lost	1	YES	NO
26	Stolen	6	NO	NO
27	Stolen	0	YES	NO
28	Stolen	21	NO	NO
29	Stolen	34	NO	YES

<sup>41</sup> UTD = Unable To Determine. The DEA Board of Professional Conduct file did not indicate whether the case was referred to the Office of Professional Responsibility.

<b>Number</b>	<b>Loss Type</b>	<b>Days Between Incident and DEA Form 29 Submittal</b>	<b>Timely Submittal of DEA Form 29</b>	<b>Referred to DEA Office of Professional Responsibility</b>
30	Stolen	1	YES	YES
31	Lost	6	NO	YES
32	Lost	7	NO	YES
33	Lost	15	NO	NO
34	Stolen	5	NO	YES
35	Lost	0	YES	YES
36	Stolen	3	YES	YES
37	Stolen	3	YES	YES
38	Stolen	31	NO	YES
39	Stolen	11	NO	YES
40	Stolen	0	YES	UTD
41	Stolen	0	YES	UTD
42	Stolen	20	NO	UTD
43	Stolen	0	YES	UTD
44	Stolen	31	NO	UTD
45	Stolen	31	NO	UTD
46	Stolen	31	NO	UTD
47	Stolen	3	YES	UTD
48	Stolen	3	YES	UTD
49	Stolen	2	YES	YES
50	Lost	2	YES	YES
51	Stolen	8	NO	NO
52	Stolen	8	NO	NO
53	Lost	4	NO	YES
54	Lost	3	YES	NO
55	Stolen	24	NO	UTD
56	Stolen	2	YES	YES
57	Stolen	37	NO	YES
58	Stolen	37	NO	YES
59	Lost	36	NO	YES
60	Stolen	3	YES	UTD
61	Stolen	2	YES	UTD
62	Stolen	2	YES	UTD
63	Stolen	20	NO	UTD
64	Stolen	2	YES	NO

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
65	Stolen	1	YES	UTD
66	Stolen	0	YES	YES
67	Stolen	1	YES	YES
68	Stolen	4	<b>NO</b>	YES
69	Stolen	2	YES	YES
70	Stolen	2	YES	YES
71	Stolen	1	YES	YES
72	Stolen	1	YES	YES
73	Stolen	2	YES	YES
74	Lost	<b>88</b>	<b>NO</b>	<b>NO</b>
75	Lost	<b>14</b>	<b>NO</b>	YES
76	Stolen	1	YES	YES
77	Stolen	1	YES	YES
78	Stolen	3	YES	UTD
79	Stolen	2	YES	YES
80	Stolen	1	YES	<b>NO</b>
81	Stolen	<b>6</b>	<b>NO</b>	YES
82	Stolen	<b>1</b>	YES	<b>NO</b>
83	Stolen	0	YES	YES
84	Stolen	0	YES	YES
85	Stolen	2	YES	YES
86	Stolen	<b>27</b>	<b>NO</b>	YES
87	Lost	0	YES	YES
88	Lost	1	YES	YES
89	Lost	0	YES	YES
90	Stolen	<b>5</b>	<b>NO</b>	UTD
91	Lost	0	YES	YES

Source: OIG analysis of the DEA Board of Professional Conduct case files

This page intentionally left blank.

## ANALYSIS OF LOST AND STOLEN DEA LAPTOPS

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
1	Lost	UTD	UTD	UTD
2	Lost	UTD	UTD	UTD
3	Lost	UTD	UTD	UTD
4	Lost	UTD	UTD	UTD
5	Lost	UTD	UTD	YES
6	Lost	UTD	UTD	UTD
7	Lost	0	YES	UTD
8	Lost	UTD	UTD	UTD
9	Lost	UTD	UTD	UTD
10	Lost	UTD	UTD	UTD
11	Lost	UTD	UTD	UTD
12	Lost	UTD	UTD	UTD
13	Lost	UTD	UTD	UTD
14	Lost	UTD	UTD	UTD
15	Lost	UTD	UTD	UTD
16	Lost	UTD	UTD	UTD
17	Lost	UTD	UTD	UTD
18	Lost	UTD	UTD	UTD
19	Lost	UTD	UTD	UTD
20	Lost	UTD	UTD	UTD
21	Lost	UTD	UTD	UTD
22	Lost	UTD	UTD	UTD
23	Lost	UTD	UTD	UTD
24	Lost	<b>1376</b>	<b>NO</b>	<b>UTD</b>
25	Lost	3	YES	UTD
26	Lost	UTD	UTD	UTD
27	Lost	UTD	UTD	UTD
28	Lost	UTD	UTD	UTD
29	Lost	UTD	UTD	UTD
30	Lost	UTD	UTD	UTD
31	Lost	UTD	UTD	UTD
32	Lost	UTD	UTD	UTD
33	Lost	UTD	UTD	UTD
34	Lost	UTD	UTD	UTD
35	Lost	UTD	UTD	UTD
36	Lost	<b>734</b>	<b>NO</b>	<b>UTD</b>
37	Stolen	<b>6</b>	<b>NO</b>	<b>UTD</b>
38	Lost	UTD	UTD	UTD

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
39	Stolen	6	NO	UTD
40	Lost	UTD	UTD	UTD
41	Lost	UTD	UTD	UTD
42	Lost	UTD	UTD	UTD
43	Lost	UTD	UTD	UTD
44	Lost	UTD	UTD	UTD
45	Lost	UTD	UTD	UTD
46	Lost	UTD	UTD	UTD
47	Lost	UTD	UTD	UTD
48	Lost	UTD	UTD	UTD
49	Lost	UTD	UTD	UTD
50	Lost	UTD	UTD	UTD
51	Lost	UTD	UTD	UTD
52	Lost	UTD	UTD	UTD
53	Lost	UTD	UTD	UTD
54	Lost	UTD	UTD	UTD
55	Lost	UTD	UTD	UTD
56	Stolen	30	NO	UTD
57	Lost	UTD	UTD	UTD
58	Lost	UTD	UTD	UTD
59	Lost	UTD	UTD	UTD
60	Lost	UTD	UTD	UTD
61	Lost	UTD	UTD	UTD
62	Lost	UTD	UTD	UTD
63	Lost	UTD	UTD	UTD
64	Lost	UTD	UTD	UTD
65	Lost	UTD	UTD	UTD
66	Lost	53	NO	UTD
67	Lost	UTD	UTD	UTD
68	Lost	UTD	UTD	UTD
69	Lost	UTD	UTD	UTD
70	Lost	UTD	UTD	UTD
71	Lost	UTD	UTD	UTD
72	Lost	UTD	UTD	UTD
73	Lost	UTD	UTD	UTD
74	Lost	UTD	UTD	UTD
75	Lost	UTD	UTD	UTD
76	Lost	2	YES	UTD
77	Lost	UTD	UTD	UTD
78	Stolen	1190	NO	UTD
79	Lost	1727	NO	UTD



Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
80	Lost	UTD	UTD	UTD
81	Lost	UTD	UTD	UTD
82	Lost	UTD	UTD	UTD
83	Lost	UTD	UTD	UTD
84	Lost	UTD	UTD	UTD
85	Lost	UTD	UTD	UTD
86	Lost	UTD	UTD	UTD
87	Lost	UTD	UTD	UTD
88	Lost	UTD	UTD	UTD
89	Lost	UTD	UTD	UTD
90	Lost	UTD	UTD	UTD
91	Lost	UTD	UTD	UTD
92	Lost	UTD	UTD	UTD
93	Lost	UTD	UTD	UTD
94	Lost	UTD	UTD	UTD
95	Lost	UTD	UTD	UTD
96	Lost	UTD	UTD	UTD
97	Lost	UTD	UTD	UTD
98	Lost	UTD	UTD	UTD
99	Lost	UTD	UTD	UTD
100	Lost	UTD	UTD	UTD
101	Lost	UTD	UTD	UTD
102	Lost	UTD	UTD	UTD
103	Stolen	0	YES	UTD
104	Lost	<b>4</b>	<b>NO</b>	<b>UTD</b>
105	Stolen	<b>50</b>	<b>NO</b>	<b>UTD</b>
106	Lost	UTD	UTD	UTD
107	Stolen	UTD	UTD	YES
108	Stolen	3	YES	UTD
109	Lost	UTD	UTD	UTD
110	Lost	UTD	UTD	UTD
111	Lost	UTD	UTD	UTD
112	Lost	UTD	UTD	UTD
113	Lost	UTD	UTD	UTD
114	Lost	UTD	UTD	UTD
115	Lost	UTD	UTD	UTD
116	Lost	UTD	UTD	UTD
117	Lost	UTD	UTD	UTD
118	Lost	UTD	UTD	UTD
119	Lost	UTD	UTD	UTD
120	Lost	UTD	UTD	UTD

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
121	Lost	UTD	UTD	UTD
122	Lost	UTD	UTD	UTD
123	Lost	UTD	UTD	UTD
124	Lost	UTD	UTD	UTD
125	Lost	UTD	UTD	UTD
126	Lost	UTD	UTD	UTD
127	Lost	UTD	UTD	UTD
128	Lost	UTD	UTD	UTD
129	Lost	UTD	UTD	UTD
130	Lost	UTD	UTD	UTD
131	Lost	UTD	UTD	UTD
132	Lost	UTD	UTD	UTD
133	Lost	UTD	UTD	UTD
134	Lost	UTD	UTD	UTD
135	Lost	UTD	UTD	UTD
136	Lost	UTD	UTD	UTD
137	Lost	UTD	UTD	UTD
138	Lost	UTD	UTD	UTD
139	Lost	UTD	UTD	UTD
140	Lost	UTD	UTD	UTD
141	Lost	UTD	UTD	UTD
142	Lost	UTD	UTD	UTD
143	Lost	UTD	UTD	UTD
144	Lost	UTD	UTD	UTD
145	Lost	UTD	UTD	UTD
146	Lost	UTD	UTD	UTD
147	Lost	UTD	UTD	UTD
148	Lost	UTD	UTD	UTD
149	Lost	UTD	UTD	UTD
150	Stolen	<b>30</b>	<b>NO</b>	<b>UTD</b>
151	Lost	UTD	UTD	UTD
152	Lost	UTD	UTD	UTD
153	Lost	UTD	UTD	UTD
154	Lost	UTD	UTD	UTD
155	Stolen	<b>15</b>	<b>NO</b>	<b>UTD</b>
156	Stolen	<b>8</b>	<b>NO</b>	<b>UTD</b>
157	Lost	<b>42</b>	<b>NO</b>	<b>UTD</b>
158	Lost	<b>42</b>	<b>NO</b>	<b>UTD</b>
159	Lost	<b>42</b>	<b>NO</b>	<b>UTD</b>
160	Lost	<b>42</b>	<b>NO</b>	<b>UTD</b>
161	Lost	<b>42</b>	<b>NO</b>	<b>UTD</b>

<b>Number</b>	<b>Loss Type</b>	<b>Days Between Incident and DEA Form 29 Submittal</b>	<b>Timely Submittal of DEA Form 29</b>	<b>Referred to DEA Office of Professional Responsibility</b>
162	Lost	42	NO	UTD
163	Lost	42	NO	UTD
164	Lost	42	NO	UTD
165	Lost	42	NO	UTD
166	Lost	42	NO	UTD
167	Lost	42	NO	UTD
168	Lost	42	NO	UTD
169	Lost	42	NO	UTD
170	Lost	42	NO	UTD
171	Lost	42	NO	UTD
172	Lost	UTD	UTD	UTD
173	Lost	UTD	UTD	UTD
174	Lost	UTD	UTD	UTD
175	Stolen	UTD	UTD	UTD
176	Stolen	10	NO	UTD
177	Lost	UTD	UTD	UTD
178	Lost	UTD	UTD	UTD
179	Stolen	46	NO	UTD
180	Stolen	6	NO	UTD
181	Lost	UTD	UTD	UTD
182	Lost	UTD	UTD	UTD
183	Stolen	25	NO	UTD
184	Stolen	34	NO	UTD
185	Lost	UTD	UTD	UTD
186	Lost	5	NO	UTD
187	Stolen	19	NO	UTD
188	Stolen	9	NO	UTD
189	Lost	UTD	UTD	UTD
190	Stolen	116	NO	UTD
191	Stolen	76	NO	UTD
192	Lost	7	NO	UTD
193	Lost	UTD	UTD	UTD
194	Stolen	29	NO	UTD
195	Stolen	UTD	UTD	UTD
196	Lost	UTD	UTD	UTD
197	Lost	UTD	UTD	UTD
198	Lost	75	NO	UTD
199	Lost	75	NO	UTD
200	Lost	75	NO	UTD
201	Lost	75	NO	UTD
202	Lost	75	NO	UTD

Number	Loss Type	Days Between Incident and DEA Form 29 Submittal	Timely Submittal of DEA Form 29	Referred to DEA Office of Professional Responsibility
203	Lost	75	NO	UTD
204	Lost	2	YES	UTD
205	Lost	UTD	UTD	UTD
206	Lost	UTD	UTD	UTD
207	Lost	UTD	UTD	UTD
208	Lost	UTD	UTD	UTD
209	Lost	UTD	UTD	UTD
210	Lost	UTD	UTD	UTD
211	Lost	UTD	UTD	UTD
212	Lost	UTD	UTD	UTD
213	Lost	UTD	UTD	UTD
214	Lost	UTD	UTD	UTD
215	Lost	UTD	UTD	UTD
216	Lost	UTD	UTD	UTD
217	Lost	UTD	UTD	UTD
218	Stolen	3	YES	UTD
219	Lost	UTD	UTD	UTD
220	Lost	UTD	UTD	UTD
221	Lost	UTD	UTD	UTD
222	Lost	495	NO	UTD
223	Stolen	UTD	UTD	UTD
224	Lost	UTD	UTD	UTD
225	Lost	75	NO	UTD
226	Lost	UTD	UTD	UTD
227	Lost	0	YES	UTD
228	Lost	0	YES	UTD
229	Lost	236	NO	UTD
230	Lost	36	NO	UTD
231	Lost	UTD	UTD	UTD

Source: OIG analysis of the DEA Board of Professional Conduct case files

## LOST AND STOLEN DEA WEAPONS NOT FOUND IN THE NCIC DATABASE

Number	Make	Model	Caliber
1	Smith & Wesson	10	38
2	Sig Sauer	P-225	9mm
3	Glock	22	40
4	Glock	19	9mm
5	Sig Sauer	P-229	40
6	Sig Sauer	P-220	45
7	Colt	M-4 Carbine	5.56mm
8	Glock	22	40
9	Glock	23	40
10	Glock	27	40
11	Glock	22	40
12	Sig Sauer	P-220	45
13	Glock	27	40
14	Sig Sauer	P-229	40
15	Glock	26	9mm
16	Remington	870	12
17	Glock	19	9mm
18	Sig Sauer	P-229	40

Source: OIG analysis of NCIC database queries

This page intentionally left blank.

## DEA-OWNED WEAPONS AND LAPTOP COMPUTERS TESTED

Location	Weapons			Laptops		
	Number Tested	Universe	Percent Tested	Number Tested	Universe	Percent Tested
DEA headquarters	388	388	100%	2,189	2,189	100%
Firearms Training Unit	3,322	3,322	100%	554	554	100%
Chicago	101	367	28%	30	108	28%
Denver	41	151	27%	19	69	28%
Houston	78	293	27%	56	205	27%
Los Angeles	171	628	27%	59	217	27%
Miami	102	386	26%	39	141	28%
New York	128	472	27%	61	224	27%
<b>TOTAL<sup>42</sup></b>	<b>4,331</b>	<b>6,007</b>	<b>72%</b>	<b>3,007</b>	<b>3,707</b>	<b>81%</b>

Source: OIG summary of DEA weapons and laptop computers tested

---

<sup>42</sup> This table summarizes the percentage of weapons and laptops tested in comparison to the universes of weapons and laptops at the locations that the OIG visited. The DEA's overall total universes were 14,449 DEA-owned weapons and 7,381 DEA-owned laptops.

This page intentionally left blank.





This page intentionally left blank.

## DEA FORM 17 FIREARMS CONTROL RECORD

U.S. DEPARTMENT OF JUSTICE - DRUG ENFORCEMENT ADMINISTRATION				
<b>FIREARMS CONTROL RECORD</b>				
MANUFACTURER	MODEL	CALIBER	WEAPON TYPE	SERIAL NUMBER
CUSTODIAN'S NAME: <i>(Last, First, Middle Initial) or OFFICE USE</i>		CUSTODIAN'S OFFICE	CUSTODIAN'S DIVISION	
CUSTODIAN'S SIGNATURE		CUSTODIAN'S SSN	DATE	
WEAPON PREVIOUSLY ISSUED TO			PREVIOUS CUSTODIAN'S OFFICE	
<p><b>INSTRUCTIONS:</b></p> <ul style="list-style-type: none"> <li>▶ This form must be completed in its entirety whenever a DEA owned weapon changes custodians. If the custodian has not changed, only the top 3 lines need to be completed.</li> <li>▶ All entries should be made in ink. Rubber signature stamps are prohibited.</li> <li>▶ Weapon serial numbers should be copied from the frame and must include any prefixes and suffixes.</li> <li>▶ Primary firearms instructors should submit the original to the Office of Training, Firearms Training Unit. A copy should be maintained in the division where the firearm is located. A copy should be provided to the agent to whom the weapon is assigned, if applicable.</li> <li>▶ Refer to Agent's Manual, Section 6122 for additional information.</li> </ul>				
PROPERTY CUSTODIAL ASSISTANT (Type or print name)	SIGNATURE OF PROPERTY CUSTODIAL ASSISTANT		DATE	
FORM DEA-17 (6-02) <i>Previous edition is obsolete</i>			Electronic Form Designed In JetForm 5.2 Version	

This page intentionally left blank.

## DEA FORM 29 PERSONAL PROPERTY NEGLIGENCE/LIABILITY ASSESSMENT

U.S. Department of Justice Drug Enforcement Administration		<b>PERSONAL PROPERTY NEGLIGENCE/LIABILITY ASSESSMENT</b>	
<b>PART I. To be completed and signed by employee. Upon completion, have supervisor sign. Forward Parts 1 through 6 to SAC, CA, or Headquarters Office Head, as appropriate. Retain Part 7 for your record.</b>			
DIVISION AND OFFICE NAME		EMPLOYEE'S NAME	
EMPLOYEE'S TITLE		SOCIAL SECURITY NUMBER	
<b>PROPERTY CATEGORY (CHECK)</b> <input type="checkbox"/> OFFICIAL GOVT. VEHICLE (OOV) <input type="checkbox"/> BADGE/IDENTIFICATION/BUILDING PASS <input type="checkbox"/> WEAPON <input type="checkbox"/> TECHNICAL EQUIPMENT <input type="checkbox"/> COMMUNICATIONS EQUIPMENT <input type="checkbox"/> ADMIN. FURN./EQUIPMENT <input type="checkbox"/> PROTECTIVE EQUIPMENT <input type="checkbox"/> OTHER (EXPLAIN BELOW)	<b>PROPERTY WAS (CHECK)</b> <input type="checkbox"/> DEA OWNED <input type="checkbox"/> RENTED <input type="checkbox"/> BORROWED <input type="checkbox"/> LEASED <input type="checkbox"/> SEIZED (NOT FORFEITED) <input type="checkbox"/> FORFEITED	<b>INCIDENT REPORTED TO POLICE</b> <input type="checkbox"/> YES <input type="checkbox"/> NO  <b>POLICE REPORT ATTACHED</b> <input type="checkbox"/> YES <input type="checkbox"/> NO  NCIC Report Date _____  NCIC NO. _____	<b>PROPERTY WAS (CHECK)</b> <input type="checkbox"/> LOST <input type="checkbox"/> STOLEN <input type="checkbox"/> DESTROYED <input type="checkbox"/> SHORT ON INVENTORY <input type="checkbox"/> DAMAGED <input type="checkbox"/> OTHER (EXPLAIN BELOW)
PROVIDE COMPLETE ITEM DESCRIPTION/NOMENCLATURE (INCLUDE DEA SERIAL NO., ETC.)			
EMPLOYEE'S STATEMENT/COMMENTS (ATTACH REQUIRED REPORTS, INCLUDING DEA-9, IF APPROPRIATE.) IF MORE SPACE IS NEEDED, CONTINUE ON PLAIN PAPER AND ATTACH APPROPRIATE NUMBER OF COPIES.			
EMPLOYEE'S NAME (TYPED)		SIGNATURE	DATE
SUPERVISOR'S NAME (TYPED)		SIGNATURE	DATE
<b>PART II. To be completed by investigator and appropriate official. Forward Parts 1 through 5 to Board of Professional Conduct (BC). Retain Part 6 for property record.</b>			
Property Acquisition Cost: \$ _____		Property Acquisition Date: _____	
RESULTS OF INVESTIGATION			
INVESTIGATOR'S NAME AND TITLE (TYPED)		SIGNATURE	DATE
REVIEWED BY: SAC/CA/NO. OFFICE HEAD (TYPED NAME)		SIGNATURE	DATE
FOR BC USE ONLY			
BC NO. _____		DEPRECIATED VALUE \$ _____	
NUMBER OF PRIOR LOSSES DOCUMENTED BY P4 _____		DATE: _____	
DEA Form (Apr. 1989) - 29		Previous editions are obsolete.	
		1-BC	

This page intentionally left blank.


## DEA FORM 171a EMPLOYEE CLEARANCE RECORD

U.S. DEPARTMENT OF JUSTICE - DRUG ENFORCEMENT ADMINISTRATION			
EMPLOYEE CLEARANCE RECORD			
(READ instructions BEFORE COMPLETING.)			
NAME OF EMPLOYEE (Last, First, MI)		POSITION (Title, Series, Grade)	EMPLOYEE'S OFFICE & DUTY STATION
FORWARDING ADDRESS (No., Street, Apt. No., City, State, Zip Code)		EFFECTIVE DATE OF SEPARATION OR TRANSFER	NEXT DUTY STATION
TYPE OF ACTION (X) ONE: <input type="checkbox"/> Resignation <input type="checkbox"/> Retirement <input type="checkbox"/> Transfer <input type="checkbox"/> Other (Specify)			
SECURITY ACTIVITY	SIGNATURE and TITLE of Individual Verifying Status of funds, Receiving Property & Initiating Debriefing	DATE	
1. Badges, Credentials			
2. Confidential/Secret (Debrief upon Transfer or Separation) SF-312			
3. Cryptographic (Debrief upon Transfer or Separation) DEA-56			
4. Sensitive Compartment Information (Debrief upon Transfer or Separation) 4355			
5. Delete M204 Access (Upon Transfer or Separation/User ID Removed)			
6. Merlin Access (Password/User ID Removed)			
7. Building Identification Pass/Keys (DEA/FBI)			
8. Weapons (Serial Number)			
9. Security Keys (Upon Transfer or Separation)			
10. Change Combination Locks			
11. Classified Documents (Turn-in upon Transfer or Separation)			
OTHER ACTIVITIES			
1. DEA Investigative Files			
2. Investigative/Technical Equipment (Pagers, cell phones, etc.)			
3. Financial Disclosure Report - SF-278			
4. Credit Cards - Telephone			
5. Credit Cards - Gasoline			
6. Medical Records			
7. Passport, Official and/or Diplomatic			
8. DEA Parking Permit			
9. Library Materials/Books			
10. Evidence Room			
11. DEA-TRANSIT SUBSIDY PROGRAM (Form DEA-392)			
FINANCE ACTIVITY			
1. Imprest Funds			
2. Credit Cards (Travel)			
3. Travel Advance			
4. Other Debt			
PROCUREMENT ACTIVITY			
1. Credit Card - Purchase			
2. Contracting Authority/Warrant (Rescind upon Transfer or Separation)			
IMMEDIATE SUPERVISOR			
1. Firebird Account/Firebird E-Mail (Password/User ID Removed)			
2. Personal Custody Property			
3. Access Keys			
4. Obligated Services (Training, PCS, etc.)			
5. Advanced Annual Leave, No. of Hours: _____			
6. Advanced Sick Leave, No. of Hours: _____			
7. FFS Access (User ID removed upon Transfer or Separation)			
REMARKS			
<p><b>CERTIFICATION OF EMPLOYEE:</b> I certify that I am familiar with and have received a copy of DOJ's fact sheet, "The Ethics in Government Act of 1978 and the Department's Standards of Conduct Regulations." I am aware of Title 18, United States Code "Crime and Criminal Procedure" which prescribes penalties for unauthorized disclosure of information relating to the national defense, and I have returned all classified documents and materials to the proper authority. I will not communicate or transmit classified information to any unauthorized person or agency. I have no other Government property, correspondence or records, and have turned in all outstanding fiscal accounts and money. I am not indebted to the U.S. Government regarding my employment with DEA.</p>			
EMPLOYEE SIGNATURE _____		DATE _____	
CLEARANCE OFFICIAL CERTIFICATION (X one)			
<p>____ I certify that all required clearances have been obtained for the above-named employee and that his/her final salary and lump sum check(s) may be released.</p> <p>____ I certify that all required clearances have <u>not</u> been obtained for the above-named employee. This matter has been referred to the appropriate finance office for recovery action pursuant to 5 U.S. C. 5512 as amended.</p>			
CLEARANCE OFFICIAL SIGNATURE _____		DATE _____	
TITLE _____		OFFICE _____	
FORM DEA-171a (9-02) Previous editions are obsolete		Electronic Forms Version Designed in JetForm 5.2 Version	

This page intentionally left blank.



## DEA FORM 609 REQUEST FOR AUTHORITY TO CARRY A PERSONALLY OWNED FIREARM

	U.S. DEPARTMENT OF JUSTICE - DRUG ENFORCEMENT ADMINISTRATION <b>REQUEST FOR AUTHORITY TO CARRY A PERSONALLY OWNED FIREARM</b>	DATE
TO	FROM <b>PRIMARY FIREARMS INSTRUCTOR</b>	
<p>Request for approval is hereby made to carry a personally owned weapon while conducting the duties of a Special Agent. This request is made pursuant to 6122.32 of the Agent's Manual.</p>		
<b>DESCRIPTION OF WEAPON</b>		
MAKE	MODEL	
SERIAL NUMBER	CALIBER	
NAME OF SPECIAL AGENT	SIGNATURE OF SPECIAL AGENT	
<p>I have inspected the above described weapon on _____ and found it to be in safe operating condition. The above agent qualified with this weapon on _____ with a score of _____. The above agent has demonstrated a thorough knowledge of the operation of the above described weapon.</p> <p>This weapon appears on the DEA approved personally owned weapon list (6122.32).</p>		
_____ FIREARMS INSTRUCTOR		
<p>In accordance with 6122.32 of the Agent's Manual, you are hereby granted authority to carry the above described weapon in the performance of official duties per DEA regulations.</p>		
APPROVED SAC/RD/HOH	DATE	
<hr/>		
FORM DEA-609 (7-02)	Electronic Forms Version Designed In JetForm 5.3 Version	

This page intentionally left blank.

## DRUG ENFORCEMENT ADMINISTRATION RESPONSE



**U. S. Department of Justice**  
Drug Enforcement Administration

[www.dea.gov](http://www.dea.gov)

Washington, D.C. 20537

**MAR 19 2008**

MEMORANDUM

TO: Raymond J. Beaudet  
Assistant Inspector General  
for ALÉil  
Office of the Inspector General

FROM: Gary W. Oetjen  
Deputy Chief Inspector  
Office of Inspections

A handwritten signature in black ink, appearing to read "Gary W. Oetjen", written over the typed name and title.

SUBJECT: DEA's Response to the OIG's Draft Report: *The Drug Enforcement Administration's Control over Weapons and Laptop Computers Follow-up Audit*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ), Office of the Inspector General's (OIG) draft audit report, entitled: *The Drug Enforcement Administration's Control over Weapons and Laptop Computers Follow-up Audit*. DEA acknowledges OIG for its efforts in conducting a review of DEA's control over weapons and laptops. As a result of this review, DEA concurs with six of the seven recommendations promulgated in the draft report and will take the necessary steps to implement the recommendations.

DEA appreciates that OIG noted the DEA made significant improvement in its rate of loss for laptop computers, decreasing by more than 50 percent, compared to OIG's 2002 audit of DEA's weapons and laptops. OIG also noted in its report that the DEA's Firearms Training Unit (TRDG) corrected all weapons-related deficiencies directed to TRDG in OIG's 2002 audit report.

OIG reported during its current review that DEA was not accurately reporting lost/stolen weapons and that all lost/stolen weapons were not entered into the National Crime Information Center (NCIC) database. In April 2007, DEA implemented a new policy regarding the loss/theft of firearms and has since ensured that all lost/stolen weapons are accurately reported and entered into the NCIC database.

OIG noted in its review that DEA was unable to provide assurance that the contents for 226 of 231 lost or stolen laptops did not contain sensitive information or personally identifiable information (PII). Moreover, OIG stated that this finding was similar to the findings in its 2002 audit report.

DEA notes that PII was federally codified in May 2006, in an Office of Management and Budget (OMB) memorandum (06-15), entitled: *Safeguarding Personally Identifiable Information*. In October 2006, DEA issued a broadcast message to all DEA employees requiring them to report losses of PII. OIG's recent review, which covered the period from January 2002 to June 2007, implies that DEA was deficient in its reporting of PII during their current and previous review when, in fact, DEA was not required to report PII until May 2006.

DEA provides the following response to the OIG's recommendations:

**Recommendation 1. Ensure that all DEA Forms 29 submitted are complete, accurate, and promptly submitted in accordance with DEA policy.**

DEA concurs with the recommendation. DEA has recently implemented new interim policy, (pending revision of DEA's Information Technology Rules of Behavior) regarding lost/stolen/missing DEA owned laptop computers by all DEA personnel, Task Force Officers (TFO) and contractors (Attachment 1). The new policy supersedes the memorandum issued by former Administrator Asa Hutchinson, dated October 18, 2002, entitled: "Improving Inventory Controls of Laptop Computers," which had been DEA's policy for the reporting of lost/stolen/missing laptop computers. The new interim policy will be incorporated into DEA's Interim Information Technology Rules of Behavior and the Administrative Manual.

The new laptop policy requires that immediate verbal notification be made to the Special Agent in Charge (SAC), Regional Director (RD), or Headquarters Office Head (HOH) by the individual who had custody or control of the laptop computer at the time of the loss/theft or who becomes aware that any laptop computer is unaccounted for or missing. The SAC/RD/HOH, or their designee, is responsible for the immediate telephonic reporting of the loss/theft of the laptop computer to the DEA Headquarters (HQ) Command Center (OMC). Within 48 hours after the discovery of the loss/theft, the SAC/RD/HOH will notify the Chief Inspector (IG), the Office of Security Programs (IS), Office of Professional Responsibility (OPR), the Office of Administration (SA), the Office of Information Systems (SI), and the Board of Professional Conduct (HRB) via a teletype or memorandum of the loss/theft. The person reporting the lost/stolen or missing laptop computer must complete the DEA Form 29 within five business days of discovering the lost/stolen or missing laptop computer. The OPR Inspector or Field Supervisory Special Agent assigned the loss/theft investigation will review the DEA Form 29 during the course of their investigation to ensure the form contains all necessary information.

In April 2007, DEA implemented new policy regarding the loss or theft of firearms. The reporting of a lost or stolen firearm mirrors the above-mentioned loss/theft/missing laptop computer policy with the exception of the time allowed for preparing the DEA Form 29. Presently, an individual is required to complete the form within 48 hours of discovering that the firearm is lost/stolen. The Agents Manual will be revised to change the time for completing the DEA Form 29 from 48 hours to five business days. The Agents Manual will still require immediate verbal notification by the SAC/RD/HOH, or their designee, to OMC and subsequent notification within 48 hours, via a teletype or memorandum, to OPR, HRB, and TRDG

**Recommendation 2. Ensure that weapon and laptop computer losses are accurately and promptly entered into the NCIC database.**

DEA concurs with the recommendation. DEA has recently implemented new interim policy regarding the reporting of lost/stolen/missing DEA owned laptop computers by all DEA personnel, TFOs, and contractors (Attachment 1). The new policy supersedes the memorandum issued by former Administrator Asa Hutchinson, dated October 18, 2002, entitled, "Improving Inventory Controls of Laptop Computers" which had been DEA's policy for the reporting of lost/stolen/missing laptop computers. The new interim policy will be incorporated into DEA's Interim Information Technology Rules of Behavior and the Administrative Manual.

Unlike the policy stated in former Administrator Hutchinson's 2002 memorandum, DEA's new laptop policy requires that the notification teletype or memorandum prepared by the SAC/RD/HOH within 48 hours of the loss/theft of the laptop computer document that the laptop was entered into NCIC as well as the name of the agency that entered the laptop computer into NCIC and the date entered. The new policy also requires that the NCIC entry confirmation be an attachment to the report of investigation regarding the loss/theft of the laptop.

In April 2007, DEA implemented new policy regarding the loss or theft of firearms. Since April 2007, there have been 13 incidents involving lost or stolen weapons and 12 of the weapons were entered into NCIC. The instance where the weapon's serial number was not entered into NCIC involved a TFO reporting his weapon lost on one day and finding it in his residence the following day.

**Recommendation 3. Revise the DEA Agents Manual to include procedures for actions required by DEA personnel to report lost or stolen laptop computers. At a minimum the Agents Manual should be revised to require information on laptop make, serial number, model number, NCIC record number, and a statement on the contents of the laptop and whether it contained classified, sensitive, or PII. The DEA Agents Manual should also be revised to require that the investigation of lost or stolen laptops verify the contents of any missing laptop and ensure this information is described in detail in the case file.**

DEA concurs with the recommendation. DEA has recently implemented new interim policy regarding the reporting of lost/stolen/missing DEA owned laptop computers by all DEA personnel, TFOs, and contractors (Attachment 1). The new policy supersedes the memorandum issued by former Administrator Asa Hutchinson, dated October 18, 2002, entitled, "Improving Inventory Controls of Laptop Computers" which had been DEA's policy for the reporting of lost/stolen/missing laptop computers. The new policy will not be included into the Agents Manual since laptop computers are utilized not only by Special Agents, but also Intelligence Research Specialists, Diversion Investigators, Forensic Chemists, support staff, and contractors. The interim policy will be incorporated into DEA's Interim Information Technology Rules of Behavior and the Administrative Manual.

DEA's interim policy mandates that during the immediate telephonic notification to OMC by the SAC/RD/HOH, or their designee, information supplied to OMC will include the laptop's make, model number, and serial number. Also included in the information supplied to OMC is whether any classified, sensitive but unclassified (SBU) or personal identifying information (PII) was stored on the laptop, and if so, a summary of the information stored including any risk posed by the loss or compromise of the information stored. The notification teletype or memorandum prepared by the SAC/RD/HOH within 48 hours of the loss/theft of the laptop computer will include the above-mentioned information along with facts that the laptop data was entered into NCIC, the name of the agency that entered the laptop computer into NCIC, and the date entered.

The interim policy requires that the OPR Inspector or Field Supervisory Special Agent assigned the loss/theft investigation prepare a report of investigation. This report will address various areas to include whether the laptop's use was consistent with DEA policy, confirmation of the installation of approved encryption software, and the type of information processed or stored on the laptop computer.

**Recommendation 4. Revise its policy to ensure that all laptop computers are encrypted.**

DEA does not concur with the recommendation. In early 2007, DEA's Office of Information Systems and the Office of Security Programs established a program to deploy and implement full hard-drive encryption on laptops that are used to process sensitive information. As of December 2007, laptops that process sensitive information or PII have full disk encryption implemented in compliance with the July 30, 2007 DEA Chief Information Officer (CIO) mandate. In this memorandum, the CIO stated, "Mobile computing devices are authorized to process and store PII and 'sensitive but classified' (SBU) data, provided they are encrypted with PointSec software (or other Office of Information Systems approved encryption software) and are not utilized to access the Internet." PII is primarily defined as any personal information that can be linked to an individual (i.e., names, social security numbers, dates of birth, etc), while SBU data includes such items as DEA-6s (and other investigative reports/documents), court orders, subpoenas, etc. All mobile computing devices that are used exclusively to support electronic surveillance, computer forensics, polygraph examinations, and other digital monitoring functions are exempt from the security requirements mandated above."

These exemptions are required based on attempts to load mission support applications onto laptops that were installed with the approved DEA encryption software. Problems with Global Positioning Satellite (GPS) monitoring, video surveillance, polygraphs and computer forensics were reported. Analysis of these problems revealed that the software lacks support for all the Operating Systems needed. The system partitioning requirements are impacted by loading the encryption software. The software caused video surveillance and control capabilities to be slowed down to a point of inoperability. DEA requests that the recommendation be changed to accommodate/exempt laptops supporting operational functions (such as Tracking and Monitoring, Video Surveillance, Polygraphs and Computer Forensics) that are rendered inoperable when full disk encryption is installed and implemented.

**Recommendation 5. Ensure that each division maintains supporting documentation for laptop purchases and disposals.**

DEA concurs with this recommendation. DEA will notify the field and Headquarters offices of the requirement to maintain laptop purchase and disposal documents in a centralized location in each division and headquarters office. The memorandum will be issued within 60 days of the issuance of the Final Report. The DEA Administrative Manual and the Property Management Handbook will also be revised to reflect this requirement for laptop purchase and disposal documentation.

**Recommendation 6. Prepare and submit to DOJ Justice Management Division complete and accurate semiannual Department Theft Reports regarding the loss of weapons and laptop computers and to DOJCERT incident reports regarding the loss of laptop computers.**

DEA concurs with this recommendation. Losses and thefts of government and personally-owned property sustained by DEA or DEA employees will be reported in accordance with the requirements and procedures contained in DOJ Order 2630.2A, Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures. The semiannual report will be reconciled with the appropriate DEA components in December and June, to ensure accuracy, then consolidated by the DEA Security Programs Manager for timely transmittal to the DOJ Security Officer in January and July.

Incident reports regarding the theft or loss of laptop computers will be governed by DEA's new interim policy regarding the reporting of lost/stolen/missing DEA owned laptop computers (Attachment 1). In accordance with this policy, the Office of Security Programs will receive reports of stolen, missing, or lost laptops, categorize incidents in accordance with DOJ/DEA policy, and ensure incidents are reported to DOJCERT and/or the Security and Emergency Planning Staff (SEPS) based on information sensitivity timeframes.

**Recommendation 7. Strengthen the exit processing for departing employees to ensure that documentation on the Employee Clearance Record clearly indicates specifics on remitted laptops.**

DEA concurs with this recommendation. The Office of Security Programs is drafting clearance procedures for separating and transferring employees that will include an inventory and disposition of all assigned government equipment to include full identification of remitted laptops. The clearance procedures will accompany an updated version of the DEA Form 171a (Employee Clearance Record).

Documentation detailing DEA's efforts to implement the attached action plan will be provided to the OIG on a quarterly basis, until such time that all corrective actions have been completed. If you have any questions regarding DEA's response to the OIG's recommendation, please contact Senior Inspector Michael Stanfill at 202-307-8769.

Attachment

# ATTACHMENT 1

OIG NOTE:

The DEA has identified Attachment 1 to its response as "DEA Sensitive." Therefore, it has been excluded from this report.



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

The OIG provided a draft of this audit report to the DEA for its review and comment. In its response to our report, the DEA concurred with six of our seven recommendations and provided supplementary comments regarding certain information contained in the report. Before addressing the actions necessary to resolve and close the report recommendations, we first address statements by the DEA concerning our findings that the DEA did not appropriately encrypt its laptop computers and did not know the contents of its lost and stolen laptops.

The DEA disagreed with our recommendation to revise its policy to ensure that all laptop computers are encrypted. The DEA requested that our recommendation be modified to recognize the need for an exemption for laptops supporting operational functions, such as tracking and monitoring using GPS, video surveillance, polygraph examinations, and computer forensics. The DEA stated that it has had difficulty operating software applications for these uses when employed on encrypted laptops and that these laptops are not authorized to process sensitive case information or personally identifiable information (PII).

We recognize that encryption software can sometimes cause problems in operating certain software applications. However, for several reasons, we believe that all DEA laptops should be encrypted and the DEA should work with the Department to identify a compatible encryption product for these laptops.

First, despite DEA's assertion that the laptops that were not encrypted were not authorized to process sensitive case information or PII, such laptops can and do contain such sensitive information. For example, our audit found five unencrypted laptops that contained sensitive case information or PII, including one laptop that the DEA would have exempted. Moreover, the DEA could not determine what was on 226 lost or stolen laptops and therefore was unable to ensure that the laptop contents contained no sensitive information or PII. These findings support our belief that, notwithstanding DEA policy, these laptops may process sensitive information, and that the DEA should encrypt all laptops to mitigate the possibility of loss of sensitive information and PII.

Second, we discussed the DEA's exemption policy with the Acting Director of the DOJ Information Technology Security Staff. He stated that

he believed the DEA should work with the DOJ information technology staff to find a solution to its encryption issues. We agree. Only if a solution cannot be found for the encryption issues should the DEA consider waiving the encryption requirement. In that event, the DEA needs to clearly instruct personnel that these laptops are not to be used for processing sensitive information or PII. Further, these laptops should be marked to indicate that they are not authorized for processing sensitive information or PII.

Finally, we note that the process the DEA used to waive the encryption for the laptops did not comply with DOJ policy. In February 2007, the Deputy Attorney General issued a memorandum addressing the protection of PII and other sensitive data. The memorandum delegated the authority to make a written determination that particular agency data is non-sensitive and exempt from encryption requirements to the head of the component, and limited further delegation to the component head's principal deputy. However, the DEA reported in its response that the DEA Chief Information Officer, not the Administrator or Deputy Administrator, exempted laptops used for supporting operational functions, which is contrary to the process required by the Deputy Attorney General's memorandum.

With regard to the DEA's investigation of laptop losses, the DEA response discusses our finding that it was unable to provide assurance that 226 of the 231 lost or stolen laptops did not contain sensitive information or PII. The DEA's response states that PII was federally codified in May 2006 in an OMB memorandum, and that the DEA then issued a message to all DEA employees requiring them to report losses of PII. The DEA response then states that the OIG report "implies that DEA was deficient in its reporting of PII during their current and previous review when, in fact, DEA was not required to report PII until May 2006."

First, the DEA's argument regarding when it was required to report lost laptops is not correct. Contrary to the DEA's assertion that its reporting obligation was not defined until the May 2006 OMB memorandum DOJ Order 2640.2E, "Information Technology Security," dated November 28, 2003, required that incidents that result in the loss or compromise of information shall be reported to the Department Security Officer and Department Chief Information Officer. Further, DOJ Information Technology Security Standard "Incident Response", Version 1.0, dated March 2005, required components to report all incidents of data loss to the DOJCERT.

Second, as noted in our report, the DEA did not know the contents of most of the missing or stolen laptops. All DEA laptops have the potential to be used for sensitive casework, and to contain sensitive or PII information.

Therefore, if laptops were lost or stolen, the DEA should have investigated the loss, determined what was on the laptop, and reported the loss to the Department. We believe this responsibility arose independently from, and before, the OMB memorandum in May 2006.

The following is our analysis of the DEA's response to our specific recommendations.

### **Status of Recommendations:**

**1. Resolved.** The DEA concurred with our recommendation to ensure that all DEA Forms 29 are complete, accurate, and promptly submitted in accordance with DEA policy. The DEA stated that it has implemented new interim policies regarding the reporting of both lost or stolen laptops and weapons, which require immediate verbal notification by the responsible parties to the appropriate Special Agent in Charge, Regional Director, or Headquarters Office Head. The policies also require a DEA Form 29 to be completed within a specified timeframe and to be reviewed to ensure that it contains all necessary information. The DEA also must ensure that its policy also includes notifying DOJCERT within 1 hour of an incident involving a lost or stolen laptop.

This recommendation can be closed when we receive copies of the revised Agents Manual and the Administrative Manual incorporating the guidelines specified in the new policies.

**2. Resolved.** The DEA concurred with our recommendation to ensure that weapon and laptop computer losses are accurately and promptly entered in the NCIC database. The DEA has implemented an interim policy specifying new reporting requirements regarding the entry of lost or stolen laptops and weapons in the NCIC database.

This recommendation can be closed when we receive copies of the revised DEA Interim Information and Technology Rules of Behavior and Administrative Manual incorporating the new policy governing entry of lost or stolen laptops and weapons in the NCIC database.

**3. Resolved.** The DEA concurred with our recommendation to revise the DEA Agents Manual to include procedures for actions required by DEA personnel to report lost or stolen laptop computers. The DEA stated that it has implemented a new interim policy regarding the reporting of lost, stolen, or missing DEA-owned laptops by its personnel. According to the DEA's response, this policy includes recording the laptop make, model number, and

serial number, as well as information on the NCIC entry and a summary of any sensitive or PII contained on the laptop.

This recommendation can be closed when we receive copies of the revised DEA Interim Information and Technology Rules of Behavior and Administrative Manual incorporating the new policy governing the reporting of lost, stolen or missing laptop computers.

**4. Unresolved.** The DEA did not concur with our recommendation to revise its policy and ensure that all laptop computers are encrypted. As discussed above, we believe the DEA should reconsider this issue. In order to resolve and close this recommendation, we believe the DEA should work with the DOJ information technology staff to find a solution to operating its technical programs with a DOJ-approved encryption software package.

**5. Resolved.** The DEA concurred with our recommendation to ensure that each division maintains supporting documentation for laptop purchases and disposals. The DEA stated that it revised its Administrative Manual and Property Management Handbook to require its field and headquarters offices to maintain purchase and disposal information in a centralized location.

This recommendation can be closed when we receive copies of the revised DEA Administrative Manual and Property Management Handbook incorporating this requirement.

**6. Resolved.** The DEA concurred with our recommendation to prepare and submit to DOJ Justice Management Division complete and accurate semiannual Department Theft Reports regarding the loss of weapons and laptop computers and to DOJCERT incident reports regarding the loss of laptop computers. The DEA states that it will comply with the reporting requirements of DOJ Order 2630.2A, "Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures." The DEA stated that it will reconcile its semiannual report with the appropriate DEA components to ensure accuracy in December and June, and that it will consolidate the information for timely reporting to the DOJ Security Officer in January and July. The DEA also stated that incident reports regarding the theft or loss of laptop computers will be governed by its new policy concerning the reporting of lost, stolen, or missing DEA-owned laptop computers.

This recommendation can be closed when we receive documentation supporting the implementation of the DEA's new policies for reporting

weapon and laptop losses to the DOJ and a copy of an accurate and timely-submitted semiannual Department Theft Report.

**7. Resolved.** The DEA concurred with our recommendation to strengthen the exit processing for departing employees to ensure that documentation on the Employee Clearance Record clearly indicates specifics on returned DEA laptops. The DEA stated that its Office of Security Programs is drafting clearance procedures for separating and transferring employees that will include an inventory and disposition of all assigned government equipment, including the full identification of returned laptops.

This recommendation can be closed when we receive the new employee clearance procedures, a revised DEA Form 171a (Employee Clearance Record), and documentation verifying that the new procedures have been implemented.