THE DEPARTMENT OF JUSTICE'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS SUMMARY REPORT

EXECUTIVE SUMMARY

In March 2001, the Office of the Inspector General (OIG) audited the Immigration and Naturalization Service's (INS) management of property and found, among other things, that the INS did not have adequate controls over property, including weapons. In particular, the audit noted that the INS classified more than 500 weapons as lost, missing, or stolen. After that audit, the FBI began reviewing its weapons and laptop computers and reported that many were missing. In response to the concerns about the Department's accountability for its weapons and laptop computers, the Attorney General requested that the OIG review controls over this property throughout the Department of Justice (Department). This property is sensitive in nature and its loss could result in danger to the public or could compromise national security or law enforcement activities.

The OIG, therefore, individually audited and reported on the controls over weapons and laptop computers at the Federal Bureau of Prisons (BOP), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the United States Marshals Service (USMS), referred to collectively in this summary report as the components. In total, the components reported an inventory of about 150,000 weapons and 25,000 laptop computers.[1] We examined the "life cycle" of this sensitive property at each component, ranging from purchase, receipt and assignment, physical inventories, loss reports and management response, return of equipment from separated employees, through the disposal of property. This capping report summarizes the findings of our individual component audits and analyzes the Department's actions related to accountability for weapons and laptop computers.[2]

---

[1] Since the OIG audited the INS's management of property in March 2001, we did not include it in this special review of weapons and laptop computers. However, whenever possible the results of our INS audit are incorporated in this summary report. For example, the inventory of 150,000 weapons includes the INS, but because the INS audit did not specifically include laptop computers, the inventory of 25,000 items does not include the INS.

[2] It is important to note that our results for the different components reflect somewhat different time periods, as noted in Appendix I, because the components were not always able to provide information for specific cutoff dates. The BOP, DEA, and USMS audits cover weapons and laptop computers that were reported lost, missing, or stolen between October 1999 and August 2001. The FBI audit covers weapons and laptop computers that were reported lost, missing, or stolen between October 1, 1999 and January 31, 2002. Finally, the losses shown for the INS cover property lost over an extended period, as we reported in our INS audit.

Our audits revealed substantial losses of weapons and laptop computers – collectively, the five Department components reported 775 weapons and 400 laptop computers as lost, missing, or stolen.[3]

At a minimum, law enforcement officials recovered 18 of these weapons in connection with their investigation of illegal activity. For example:

- Local police recovered a handgun stolen from an FBI agent's residence in New Orleans, Louisiana, from the pocket of a murder victim;

- Police in Atlanta, Georgia, recovered a stolen DEA weapon during a narcotics search at a suspect's residence; and

- Police in Philadelphia, Pennsylvania, and Tampa, Florida, recovered INS weapons that were used to commit armed robberies.

We were unable to determine the types of information contained in the 400 lost laptop computers because the components generally did not record the sensitivity of the information stored on the lost laptops. For example, the classification level of at least 218 lost, missing, or stolen FBI laptop computers was unknown. Due to the nature of the intelligence and law enforcement work conducted by the components, however, it is possible that the missing laptop computers would have been used to process and store national security or sensitive law enforcement information that, if divulged, could harm the public.

[3] However, these numbers do not reflect an additional 211 weapons that the FBI identified as lost, missing, or stolen as a result of an inventory that it concluded on March 31, 2002. These additional weapons were reported missing outside the scope of our audit period, in some cases many years ago. Therefore, the number of missing FBI weapons we tested and report was smaller (212) than the total number of reported FBI losses (423). If we include those weapons, the total number of reported losses for the Department is 986. Finally, the 400 laptop computers represent losses at the FBI, BOP, and USMS. The DEA was unable to determine its laptop computer losses due to the unreliability of its inventory records. In addition, our audit at the INS did not include tests specific to laptop computer losses.

COMPONENT EMPLOYEES, SENSITIVE PROPERTY, and LOSSES[4]

AGENCY	TOTAL STAFF	AGENTS OR OFFICERS[5]	TOTAL LAPTOPS	LAPTOP LOSSES	TOTAL WEAPONS	WEAPON LOSSES
BOP	33,859	32,790 [6]	2,690	27	20,594	2
DEA	9,209	4,529	6,134	Unknown [7]	14,921	16
FBI	26,748	11,193	15,077	317	49,696 [8]	212 [8]
INS	34,844	19,600	Unknown [9]	Unknown [9]	50,306	539
USMS	7,561	6,261	1,450	56	14,361	6
TOTAL	112,221	74,373	25,351	400	149,878	775

In sum, the Department reported a total of 775 missing weapons and 400 missing laptop computers during the audit periods. Apart from the INS and the FBI – who reported losses of 539 and 212 weapons, respectively – none of the three other Department components audited reported more than 16 missing weapons. With respect to laptop computers, the DEA could not provide us with the number of losses due to the unreliability of its data. The FBI reported 317 of its more than 15,000 laptop computers as missing while the USMS reported 56 of its 1,450 laptops as missing.

The Justice Management Division, the Department's administrative arm, established property management regulations that delegated property management responsibilities to the individual components. While these regulations establish minimum standards for component property management systems, they do not require Department oversight of component activities. In our judgment, the loss of 775 weapons and 400 laptop computers indicates a lack of accountability for sensitive Department property. Consequently, we believe that it is critically important

---

[4] The data appearing in this table were obtained from records provided by the components.

[5] These numbers refer to all personnel authorized to use weapons, whether categorized as a "special agent" or another title.

[6] According to the BOP, in the event of an emergency at a facility all employees who have completed firearms training (32,790) are required to respond.

[7] Due to the unreliability of its data, DEA was unable to provide us with the number of laptop computer losses it had incurred.

[8] The FBI's loss of 212 weapons represents all functional weapons reported as lost, missing, or stolen between October 1, 1999, and January 31, 2002, but does not include an additional 211 weapons that were reported lost, missing, or stolen outside the audit period. Also, while the FBI's inventory includes 3,039 training weapons, the reported 212 losses exclude lost or missing training weapons. According to the FBI's Firearms Training Unit, it is possible to restore some of these training weapons to "live-fire" capability. However, this would require the services of a skilled gunsmith and the acquisition of parts available only from the manufacturer or a licensed dealer.

[9] As discussed previously, our audit of INS property management did not include specific tests of laptop computers.

for the Department to increase its oversight role in the management of sensitive property such as weapons and laptop computers at the components. Further, we believe that the Department must take action to tighten controls that are currently weak, inadequate, or not fully implemented.

At the conclusion of our audits at each component, we made specific recommendations for improving weapon and laptop computer accountability. For example, we recommended that the components integrate or reconcile their property management and accounting systems to ensure that all purchased weapons and laptop computers are accounted for. In addition, we recommended that the components complete physical inventories as required. These recommendations generally have been well received, and in many cases corrective actions are already underway.

Based on the weaknesses we found at the Department and component levels, we offer a series of recommendations in this summary report to strengthen controls over weapons and laptop computers in an effort to reduce future losses. We believe that the Department should:

- Consult with component heads to determine if the current ratios of weapons to employees are appropriate. We found that the ratio varied from .63 weapons per employee in the BOP to 4.44 weapons per employee in the FBI.

- Revise Department credit card directives to prohibit the use of government credit cards to purchase weapons. The BOP permitted its institutions and local offices to purchase weapons using credit cards.

- Develop and implement a standard security policy for securing weapons in vehicles to reduce the number of weapon losses. At least 59 weapons were reported stolen from vehicles.

- Ensure that all types of sensitive property are within the components' definition of "controlled property." We found that the INS and USMS both had sensitive property such as stun guns, stun belts, and laptop computers that were not encompassed within the current definition. As a result, these items were not subject to physical inventory and inclusion in the official property management records, thereby increasing their susceptibility to loss.

- Require the components to inventory weapons at least annually. In addition, the Department should require components to report on the status of their physical inventory activities. At the time our audit

began in August 2001, the FBI had not completed a controlled property physical inventory since before 1993.

- Encourage components to take advantage of technological advances such as barcodes and scanning devices to enhance their management of sensitive property.

- Strengthen requirements for reporting loss of weapons and laptop computers by: (1) establishing deadlines for reporting loss of a weapon or laptop computer; (2) requiring inclusion of the loss discovery date and sensitivity of information stored on lost laptop computers; and (3) requiring timely reports of weapon and laptop computer losses to the National Crime Information Center.

- Tighten regulations requiring component review of the circumstances that caused the loss of weapons and laptop computers. A significant number of sensitive property losses have not been adjudicated by the components or reviewed in a timely manner. The timing of the reviews ranged from 6 to 588 days after losses were discovered. In addition, only 4 percent of the weapon losses and 17 percent of laptop losses have so far resulted in recommendations for disciplinary action.

- Revise the guidelines for retrieving sensitive property, such as weapons and laptop computers, from separated employees to ensure that all items are returned to component control. We found that current procedures were not effective in ensuring that these types of property were returned. In fact, in 2001 the FBI found that at least 31 weapons of separated agents could not be accounted for.

- Require that laptop computer disposal documents certify that all sensitive information has been removed before the computer is disposed. Our review of laptop computer disposal records at the components found that the majority of records at the BOP and FBI did not specify the contents of the machines or contain a certification that all sensitive information had been removed.

In conclusion, the Department's current guidelines and procedures do not provide assurance that sensitive property such as weapons and laptop computers are protected against waste, loss, and abuse. We believe it is imperative for the Department and the components to improve the accountability and control of its weapons and laptop computers to protect the public and the integrity of its law enforcement activities.

THE DEPARTMENT OF JUSTICE'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS: SUMMARY REPORT

TABLE OF CONTENTS

I. INTRODUCTION

The Department of Justice

The Department of Justice (Department), established in 1870,[10] seeks to enforce the law and defend the legal interests of the United States, provide federal leadership in preventing and controlling crime, administer and enforce the Nation's immigration laws, and ensure fair and impartial administration of justice for all Americans.

The Department is composed of law enforcement bureaus and various offices, boards, and divisions, each with its own mission, goals, and resources. The majority of the law enforcement functions are performed by five components: the Federal Bureau of Prisons (BOP), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), and the United States Marshals Service (USMS), collectively referred to in this report as the components.

Component Background

Within the Department, the components serve a myriad of purposes and assist the Department in different ways. Background information for each of the components is shown in the following table.

[10] 1870 Act to Establish the Department of Justice, ch 150, 16 Stat. 162 (28 USC § 501). The position of Attorney General, however, was created by the Judiciary Act of 1789, ch. XX, § 35, 1 Stat. 73, 93.

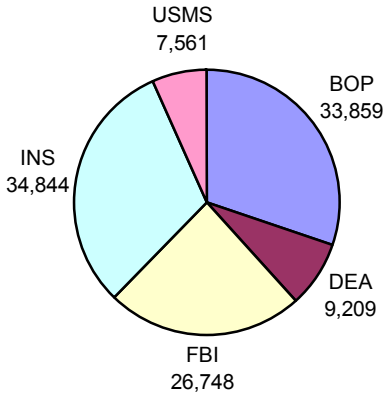
COMPONENT INFORMATION

COMPONENT & DATE ESTABLISHED	AREA OF RESPONSIBILITY/MISSION	NUMBER OF OFFICES
BOP -- 1930	To protect the public's safety by ensuring federal offenders serve their imprisonment in safe, secure, cost-efficient, humane institutions and encouraging inmates to participate in programs designed to help them adopt a crime-free lifestyle upon their return to the community.	Headquarters, 3 training centers, 103 institutions, 6 regional offices, and 29 community corrections offices
DEA -- 1973	To enforce the controlled substance laws and regulations of the U.S.	Headquarters, 1 training facility, 21 domestic offices, and 78 foreign offices
FBI -- 1909	To investigate crimes against the U.S., including counterterrorism, drugs/organized crime, foreign counterintelligence, violent crimes, and white-collar crimes.	Headquarters, 1 training facility, 56 field offices, and 47 overseas offices
INS -- 1940	To administer and enforce the nation's immigration laws.	Headquarters, 3 regional offices, 33 U.S. district offices, 3 overseas district offices, and 21 border patrol sectors
USMS -- 1789	To protect the federal courts and ensure the secure operation of the judicial system, including apprehending fugitives, protecting witnesses, and transporting prisoners.	Headquarters, 94 U.S. district offices, 1 special operations facility, and 1 training facility

Source: Component History and Organizational Documents

As the missions of the components vary, the number of employees necessary to carry out the responsibilities also varies. In total, the components employ 112,221 people, 3,443 of which are contract court security officers for the USMS; the following chart shows the relative size of each component.

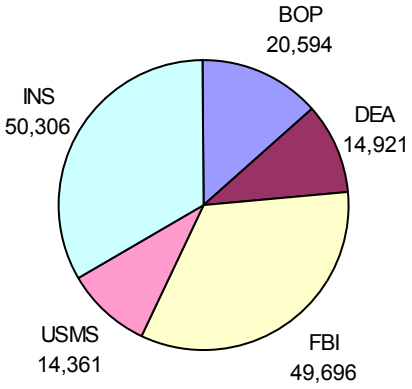
COMPONENT SIZE
(BASED ON NUMBER OF EMPLOYEES)[11]



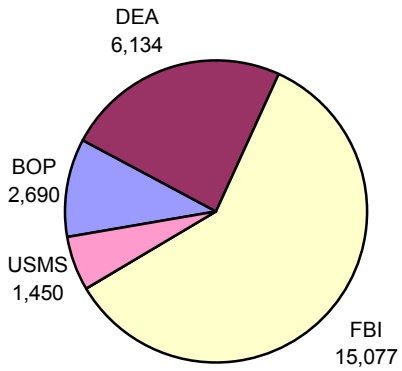
The responsibilities of the components require them to maintain an inventory of sensitive property, including weapons and laptop computers, to assist in performing their missions. Together, the components have 149,878 weapons and 25,351 laptop computers. The relative sizes of the components' inventory of weapons and laptop computers appear in the following charts.

WEAPON AND LAPTOP COMPUTER INVENTORIES

WEAPONS



LAPTOPS (excluding INS)



[11] The figures used in the charts are based upon data provided by the components; please see Appendix I for the timing of the information.

OIG Audits of Weapons and Laptop Computers in the Components

In March 2001, the Office of the Inspector General (OIG) audited the INS's management of its property and found, among other things, that the INS did not have adequate controls over property, including weapons.[12] In particular, the audit noted that the INS identified more than 500 weapons as lost, missing, or stolen. After that audit, and as a result of inquiries from the Congress and the Webster Commission,[13] the FBI reported over 400 weapons and 180 laptop computers were missing from its inventory.[14]

In response to concerns about the Department's accountability for its weapons and laptop computers, the Attorney General requested the OIG to conduct audits of the controls over the inventory of such property throughout the Department. This property is sensitive in nature and could result in danger to the public or compromise national security or law enforcement investigations if not properly controlled. We therefore conducted audits and issued separate reports on the BOP, DEA, FBI, and USMS's controls over weapons and laptop computers.[15]

Objectives

This report is a capping report that summarizes the five audits noted above, each of which was performed in accordance with Government Auditing Standards.[16] In addition, to the extent possible, we have compared and contrasted the components' policies, procedures, and practices. However, in many instances we were unable to include the INS in this analysis because the scope and methodology of that audit did not

---

[12] Audit report number 01-09, "INS Management of Property."

[13] The Commission for Review of FBI Security Programs, headed by former FBI Director William H. Webster.

[14] The FBI's report documented losses or thefts of property that occurred as long ago as ten years.

[15] Since we had completed an audit of the INS's management of property in March 2001, we did not conduct a separate review of the INS regarding its controls over weapons and laptop computers. We also did not audit the Department's litigating components because they have very few weapons.

[16] "The BOP's Control Over Weapons and Laptop Computers," Audit Report Number 02-30; "The DEA's Control Over Weapons and Laptop Computers," Audit Report Number 02-28; "The FBI's Control Over Weapons and Laptop Computers," Audit Report Number 02-27; "The INS's Management of Property," Audit Report Number 01-09; "The USMS's Control Over Weapons and Laptop Computers," Audit Report Number 02-29.

correspond to our other audits.[17] This capping report also includes an assessment of the Department's role and responsibilities regarding the controls over weapons and laptop computers. At the conclusion, we provide recommendations for improving the Department's accountability of these types of sensitive property.

[17] Our audit approach, as well as the scope and methodology utilized in the individual component audits, appears in the respective reports. If results from the INS are not included in a particular section of this capping report, it is because our data for that variable was not compatible.

II. SIGNIFICANT LOSSES OF SENSITIVE DEPARTMENT PROPERTY AND POTENTIAL PUBLIC HARM

Audits at the five components revealed substantial losses of weapons and laptop computers. During the time periods covered by our reviews, the components collectively reported losses of at least 775 weapons and 400 laptop computers.[18] However, these numbers do not reflect 211 additional weapon losses that the FBI identified as a result of an inventory that it concluded on March 31, 2002. These additional missing weapons were reported outside the scope of our audit period; in some cases many years ago. The number of FBI weapon losses we tested and report was smaller than the total losses of FBI weapons (212 rather than 423), because our audit was based on items reported missing from October 1, 1999 through January 31, 2002.

At a minimum, 18 of the weapons lost by the components were recovered by law enforcement officials in connection with their investigation of illegal activity. It is impossible to determine if the lost laptop computers contained national security or investigative information because the components generally did not record the sensitivity of information stored on the machines.

The size of the components and their inventories vary widely. The table below displays component data related to size, inventory, and reported losses.

COMPONENT EMPLOYEES, SENSITIVE PROPERTY, and LOSSES[19]

AGENCY	TOTAL STAFF	AGENTS OR OFFICERS[20]	TOTAL LAPTOPS	LAPTOP LOSSES	TOTAL WEAPONS	WEAPON LOSSES
BOP	33,859	32,790 [21]	2,690	27	20,594	2
DEA	9,209	4,529	6,134	Unknown [22]	14,921	16
FBI	26,748	11,193	15,077	317	49,696 [23]	212 [23]
INS	34,844	19,600	Unknown [24]	Unknown [24]	50,306	539
USMS	7,561	6,261	1,450	56	14,361	6
TOTAL	112,221	74,373	25,351	400	149,878	775

[18] The circumstances surrounding these losses appear in the components' individual reports.

[19] The data in this table and the ensuing discussion were obtained from records provided by the components. The time periods covered by the data vary; see Appendix I for more information.

[20] These numbers refer to all personnel authorized to use weapons, whether categorized as a "special agent" or another title.

[21] According to the BOP, in the event of an emergency at a facility, all employees who have completed firearms training (32,790) are required to respond.

[22] Due to the unreliability of its data, DEA was unable to provide us with the number of laptop computer losses it had incurred.

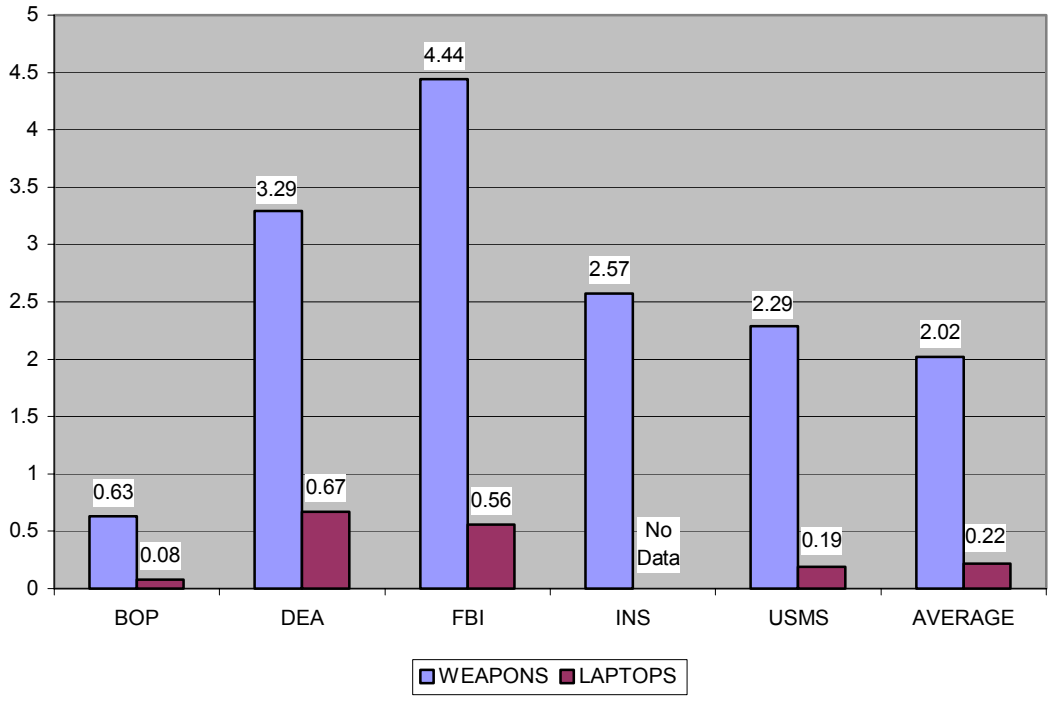
[23] The FBI's inventory includes 3,039 training weapons and the 212 reported losses exclude 142 training weapons. According to the FBI's Firearms Training Unit, it is possible to restore some to live-fire capability. However, this would require the services of a skilled gunsmith and the acquisition of parts available only from the manufacturer or a licensed gun dealer.

[24] As discussed previously, our audit of INS property management did not include specific tests of laptop computers.

The components' inventories include various types of weapons, such as revolvers, semi-automatic pistols, shotguns, rifles, sub-machine guns, and gas grenade launchers. In addition, each component's inventory contains training weapons, many of which are non-lethal.

The following graph depicts the total number of weapons and laptop computers per employee for the components and the overall average. The FBI displayed the highest weapons-to-agent/officer ratio - almost 4.5 weapons - while the component average is about 2. However, the component average is distorted by the fact that 97 percent of BOP staff is authorized to use weapons in an emergency, resulting in a weapons-to-agent/officer ratio of .63 for the agency. The average weapons-to-agent/officer ratio, excluding the BOP, is 3.11.

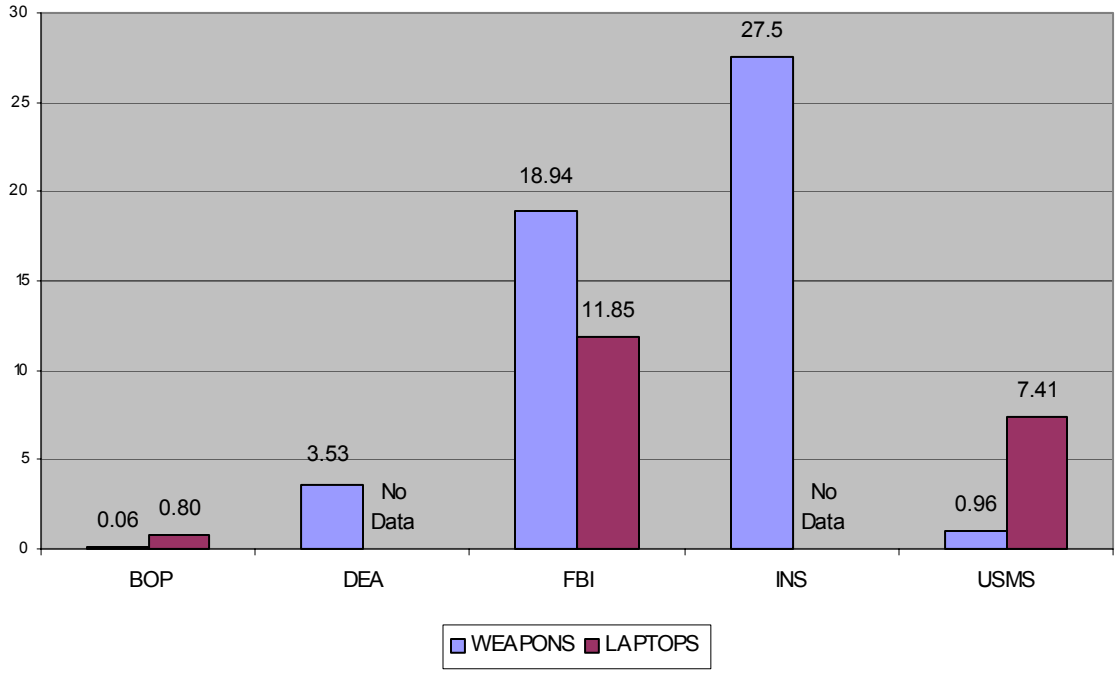
NUMBER OF WEAPONS AND LAPTOP COMPUTERS PER EMPLOYEE[25]



[25] The number of laptop computers per employee is computed using the total staff. The numbers for weapons per employee referred to on pages 7 and 8 are computed using only the number of staff authorized to utilize weapons. With respect to the USMS, the number of employees and weapons used to compute the ratio include the 3,443 contract court security officers and the USMS-owned weapons provided for their use.

In total, the components reported losses of 775 weapons and 400 laptop computers.[26] The following graph displays loss ratios by component.

RATIO OF WEAPON AND LAPTOP COMPUTER LOSSES PER 1,000 EMPLOYEES



These losses indicate a lack of accountability for sensitive property. We reviewed the circumstances surrounding the losses and, in our judgment, a significant number were avoidable through tighter controls and physical security. The circumstances of each loss are summarized in the individual reports. Our recommendations for tighter controls appear in Part V (OIG Conclusions and Recommendations).

It is important to note that our results reflect different periods in time, as noted in Appendix I. The FBI's loss of 212 weapons includes all functional weapons *reported* as lost, missing, or stolen between October 1, 1999, and January 31, 2002. Our review of these losses disclosed that many of these weapons were actually lost many years ago, but not reported until recently (see section entitled "Initial Written Reports" on page 18) because the FBI had not completed a physical inventory of property since before 1993. Similarly, the losses shown for the INS represent property lost over an extended period.

[26] These figures represent data provided to us by the components; we did not verify their accuracy.

Potential Physical Harm to the Public

At least 18 DEA, FBI, and INS weapons have been recovered by law enforcement personnel in connection with their investigation of illegal activity. These incidents are summarized below:

DEA – Four DEA weapons that were reported as lost, missing, or stolen were recovered by law enforcement agencies. Below is a summary of the circumstances of the recovery of three of the weapons; the details of the remaining firearm were unavailable.

- The Baltimore, Maryland, Police Department recovered one weapon during the arrest of an individual on a handgun violation.

- The Everett, Washington, Police Department recovered one weapon during an investigation conducted as a result of a search warrant.

- The Atlanta, Georgia, Police Department recovered one weapon during a narcotics search at a suspect's residence.

FBI – We identified five weapons[27] that were recovered by law enforcement personnel.

- Police in Memphis, Tennessee, recovered a stolen firearm when they arrested an individual for unlawful possession of a weapon.

- Two firearms were stolen from an agent's residence in Baltimore, Maryland. One weapon was recovered soon after the theft and Baltimore police retrieved the second one, a revolver, during an arrest in response to a narcotics call.

- New York City police recovered a weapon from an individual charged with criminal possession of a weapon and unlawful possession of 18 bags of marijuana.

- A handgun was stolen from an agent's residence in New Orleans, Louisiana; police officers recovered the weapon from the pocket of a murder victim.

[27] The recovery of two additional FBI weapons is discussed in the "Return of Equipment from Separated Employees" section on page 23.

INS – Our audit at the INS revealed that seven missing or stolen weapons were subsequently recovered by law enforcement agencies.

- In two separate instances, Philadelphia, Pennsylvania, police and Tampa, Florida, police recovered an INS weapon that was used to commit armed robbery.

- A Tulare County, California, law enforcement agency recovered an INS weapon in connection with a raid on an illicit drug laboratory.

- San Antonio, Texas, police recovered an INS weapon from an individual who was arrested and charged with "deadly conduct."

- New York City police confiscated an INS weapon from an individual they arrested and charged with criminal possession of a weapon.

- A Detention Enforcement Officer, within a span of four years, reported at least three INS weapons being stolen from him. According to Eloy, Arizona, police officials, two weapons were recovered, one of which was being held as evidence in a homicide investigation.

The 18 weapons noted above represent those that had been recovered at the time of our audits. However, it is conceivable that more lost weapons could be recovered during future investigation of criminal activity.

Potential Disclosure of Sensitive Information

Our audits also revealed that the BOP, FBI, and USMS lost a total of 400 laptop computers. As previously noted, DEA was unable to determine its laptop computer losses due to the unreliability of its inventory records. Further, our audit at the INS did not include tests specific to laptop computers.

We were unable to identify the types of information contained in the lost laptop computers. However, due to the nature of the law enforcement work conducted by each of the components, it is possible that the laptop computers would have been used to process and store national security or sensitive law enforcement information that, if divulged, could harm the public.

The Department's Security and Emergency Planning Staff (SEPS), an office within the Justice Management Division, maintains records of the number of laptop computers each Department component had authorized for processing classified information.[28] According to SEPS, the components had the following numbers of functioning laptop computers authorized for classified processing:

NUMBER OF CLASSIFIED LAPTOPS AT THE COMPONENTS

COMPONENT	TOP SECRET	SECRET	TOTALS
BOP	0	1	1
DEA	0	0	0
FBI	5	8,000	8,005
INS	0	10	10
USMS	0	0	0
TOTALS	**5**	**8,011**	**8,016**

It is important to note that classified information is not the only information that needs to be protected from unauthorized disclosure. The law enforcement nature of the components requires them to routinely have access to sensitive information that, if divulged, could adversely affect the ability of the components to accomplish their missions. Examples of sensitive information include the names of people under investigation, the

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

> **TOP SECRET** – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
>
> **SECRET** – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
>
> **CONFIDENTIAL** – Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. None of the components had any laptops authorized at this level.

identity of undercover agents, or information obtained during the conduct of an investigation. While not directly affecting the national security of the United States, unauthorized disclosure of sensitive information can endanger people and hamper investigations.

Officials from the BOP, DEA, FBI, and USMS told the OIG that laptop computers are used to process sensitive information. Our review of records related to the lost laptop computers revealed that for the majority of the losses, the components could not determine if sensitive data had been lost because the written loss reports did not detail the contents of the lost machines. The FBI reported to us that the classification level of at least 218 of the lost, missing, and stolen laptop computers was unknown. Further, the USMS did not require employees to record any information about the data stored on lost laptop computers.

This raises significant concerns over laptop computer losses and the possible loss of sensitive data. The Department must improve the control of laptop computers and the safeguarding of information stored on these machines. Further, if machines are lost, it is imperative that the components make a determined attempt to document their contents, including the data and related classifications.

III. WEAK CONTROLS OVER WEAPONS AND LAPTOP COMPUTERS AT ALL FIVE COMPONENTS AUDITED

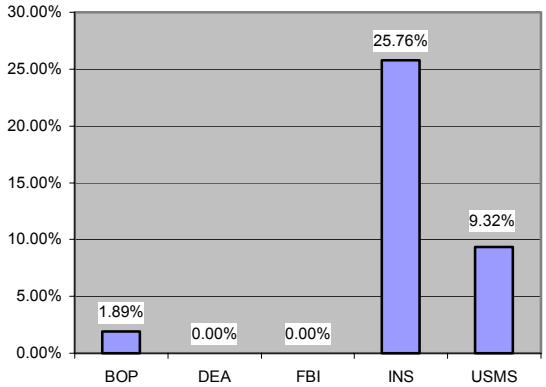
At each component, we reviewed management controls and activities related to weapons and laptop computers. Specifically, we assessed the adequacy of purchasing, receipt and assignment, physical inventories, reporting of lost items, management action in response to lost items, return of equipment from separated employees, and disposal of weapons and laptop computers. In general, we found the basic control structure was similar at each of the components. However, procedures and activities varied from component to component, oftentimes with significant effects. For example, although the FBI's internal guidelines require inventory of all controlled personal property every two years, the last complete inventory was conducted before 1993. The results of our analysis of component controls follow.

Purchasing

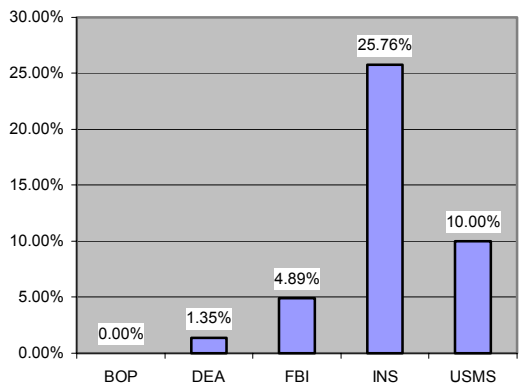
At each of the components, we reviewed a judgmental sample of purchase documents to determine if purchased property was accounted for in the official property management system. We found shortcomings in the components' recording of purchased property. The following graphs display, by component, the percentage of tested purchased property not recorded (the INS data represents all types of property, not only weapons and laptop computers).

PURCHASE TESTING RESULTS

WEAPONS SAMPLE NOT RECORDED



LAPTOPS SAMPLE NOT RECORDED



In our judgment, the failure to record property purchases in the official property records is a significant weakness because the unrecorded property is highly susceptible to loss or abuse. We believe the components can improve in this area by integrating or reconciling their accounting and property management systems.

Joint Financial Management Improvement Program (JFMIP)[29] guidelines stress the importance of integrated systems to facilitate reconciliation and improve the accuracy and completeness of all financial records. Without system integration or reconciliation, property system accuracy and completeness is reliant upon the initiative and integrity of individual property custodians to record new property acquisitions into the property system.

During our testing, we reviewed the purchasing mechanisms employed by the components. At each, laptop computer purchases were decentralized; field offices were allowed to purchase machines using purchase orders, credit cards, or other means. In contrast, weapons purchasing was centralized at the DEA, FBI, and USMS. Each of these components had a firearms unit responsible for procuring and distributing component owned weapons. This centralization was an additional control imposed due to the sensitivity of these items and may have contributed to the fact that all weapons purchases tested at the DEA and FBI were accounted for in the property management system.

Purchasing at the BOP was decentralized; institutions and local offices were allowed to purchase weapons using credit cards. We recommended that the BOP prohibit this practice to further control its weapons inventory and the BOP has initiated corrective action. This additional control is warranted because weapons are possibly the most highly sensitive type of property due to their lethal nature. We discussed the establishment of a Department-wide guideline prohibiting the use of credit cards for weapons purchases with Department officials, who agreed that such a restriction was sensible.

[29] JFMIP is a joint cooperative undertaking of the Office of Management and Budget, the General Accounting Office, the Department of Treasury, and the Office of Personnel Management. Working with operating agencies, the JFMIP strives to improve financial management practices throughout the government.

Receipt and Assignment

Policies and procedures for receiving and assigning property varied at the components.[30] To test the accuracy of system records and the receipt and assignment of property, we physically inspected a sample of property at each component. Generally, we located all selected property and noted only minor control weaknesses. None of the components' processes appeared better than the others, and therefore we do not endorse a particular system of procedures.

Protection/Security of Weapons – Our audits at the components revealed that specific policies regarding the storage of weapons varied.

Within Component Space: The most significant difference among storage policies within component space was noted between the BOP and the rest of the components. Due to the security required within BOP institutions, employees inside BOP correctional facilities are not allowed to routinely carry lethal weapons on their persons. Instead, firearms and other weapons are generally stored in a central armory. Weapons are temporarily assigned only during emergency situations or temporarily assigned to correctional officers to accomplish specific tasks such as hospital escort trips, bus transports, or target practice.

Although this stringent control may have contributed to the fact that the BOP had the lowest number and percentage of lost weapons (see charts on pages 6 and 8), it is not practical to institute this control at all components. The investigative missions of the other components require law enforcement personnel to routinely leave component space with their weapons.

Outside Component Space: The DEA, FBI, and USMS had different policies related to the storage of weapons in vehicles. The DEA had the most stringent policy: DEA regulations prohibit the storage of handguns in unattended government vehicles at any time. The FBI allows *temporary* storage of weapons in unattended vehicles, provided that the vehicle doors are locked, the firearm is contained in a secure device or container that cannot be removed easily from the vehicle, and circumstances prevent more secure storage. The FBI's policies caution that, even when properly secured, firearms should not be left in unattended vehicles overnight unless required by operational circumstances.

[30] For specific details on the policies and procedures for each component, please see the individual reports.

The USMS had the most lenient policy regarding the storage of weapons in vehicles. USMS guidelines allow for weapons to be stored in unattended vehicles as long as the vehicle is secured and the weapon is in a locked container. The policy does not set any limitations on the appropriate length of time that weapons can be stored in vehicles. Therefore, it is conceivable that weapons could be stored in vehicles for extended periods of time or even on an almost permanent basis.

Although the USMS had a minimal number of weapon losses, 3 of the 6 missing weapons were stolen from unoccupied vehicles or last seen in a vehicle. In addition, according to the DEA and FBI, at least 56 other weapons were reported stolen from vehicles. We believe that strengthening the security guidelines for weapons outside of component space could reduce the number of weapon losses.

Pooled Property and Specialized Equipment – The BOP, FBI, and USMS all had rapid response teams, each with an inventory of standard and specialized equipment to utilize in the event of an emergency. We considered this an area of importance because the extraordinary nature of these items would make them particularly harmful in the hands of the public. Generally, we found this equipment to be adequately protected and accounted for.

On September 11, 2001, we were on site at Camp Beauregard, Louisiana, when the USMS Special Operations Group received its mobilization orders to respond to the terrorist attacks. We observed the highly organized weapons storage system and their mobilization efforts. A noteworthy practice that the USMS utilized was to maintain equipment and supplies in pre-palletized, barcoded containers that could be easily transferred to a transport vehicle. As a result, the team and all needed equipment were mobilized very quickly in response to the terrorist attacks.

Physical Inventory Procedures

According to guidelines established by the Department,[31] controlled personal property is property that because of its nature must be subject to more stringent control and be physically inventoried at least biennially.[32]

---

[31] DOJ Order 2400.3, "Justice Property Management Regulations."

[32] Within the components, the terminology used to refer to controlled personal property varied slightly. In some cases, the term "accountable property" was used; for consistency and clarity, we have used the Department's term.

The Department's definition includes property: (1) costing $1,000 or more, (2) that due to its inherent attractiveness or portability is subject to a high probability of theft or misuse, or (3) that contains sensitive information or is sensitive in nature, such as weapons or communication equipment.

Within the components, the definition of controlled personal property varies. Weapons and laptop computers were generally categorized as controlled personal property, regardless of cost. However, at the time of our audit, the INS's definition of controlled personal property excluded property costing $1,000 or less,[33] even those items with data storage capability (i.e., laptop computers). Further, the USMS maintained a supply of stun guns and stun belts that were not designated as controlled personal property. These items emit electrical charges to temporarily immobilize individuals. In our judgment, policies should be revised to ensure sensitive equipment such as laptop computers at the INS and stun guns and stun belts at the USMS are subject to physical inventory and inclusion in the official property management records.

The BOP had the strongest physical inventory policy; it required all controlled personal property to be inventoried every year. The policy at the DEA, FBI, INS, and USMS was to inventory controlled personal property at least every two years. In addition, the DEA, INS, and USMS required weapons to be physically inventoried annually. We found that the BOP and USMS were generally current in their physical inventories. However, the FBI had not completed a physical inventory of controlled personal property since before 1993. In the intervening years, the FBI had attempted to conduct inventories, but these were never completed. In our judgment, the FBI's chronic failure to complete physical inventories greatly undermined its ability to manage its assets and significantly contributed to the material losses of weapons and laptop computers reported (see charts on pages 6 and 8). In addition, DEA experienced difficulties completing inventories as required.

The inventory procedures utilized at the components were generally the same, except for the USMS which conducted its inventories on a continual basis. Thus, the entire USMS is not undergoing its controlled personal property physical inventory at the same time and work in the headquarters property office can remain at a more consistent level. This consistency minimizes inaccuracies by eliminating the taxing efforts associated with conducting and reconciling a physical inventory of the entire controlled personal property universe. The method also reduces the likelihood of other property management tasks being neglected.

[33] INS policy requires all weapons to be physically inventoried, regardless of cost.

We were surprised to find the components' overall lack of use of technology to aid them in conducting their physical inventories. Barcodes and scanners have been commonly used during physical inventories in the private sector for a long time. However, there have been only minimal efforts within the components to use barcode scanners in an effort to simplify inventory procedures. The FBI was the only component to make widespread use of barcode scanners; however, officials attributed many of the physical inventory delays to technological problems encountered with barcode equipment.

Reporting of Lost and Stolen Weapons and Laptop Computers

Each of the components required missing controlled personal property to be reported at various levels both within and outside the organization. The specific procedures and timetables for communicating the details and circumstances varied from component to component.

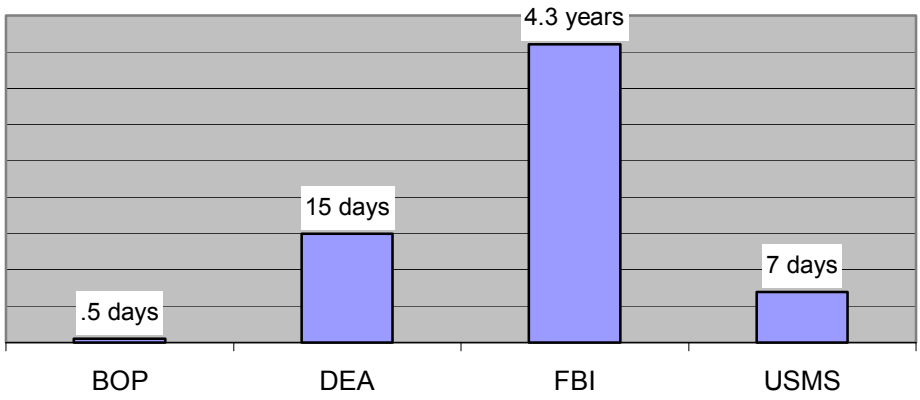
Initial Written Reports – All of the components required employees to report property losses. We found that the BOP and FBI imposed no timetable for reporting lost items, including weapons. Consequently, losses of a significant number of FBI weapons were not documented timely and initial loss reports ranged from the same day to 23 years after discovery of the loss. The average time for the loss to be reported in the FBI was 4.3 years.

Although the BOP did not have a time requirement, we did not detect severe reporting delays.[34] However, at the BOP, as well as at the DEA, FBI, and USMS, we were unable to analyze the timing of some loss reports because in many instances the documents did not provide the date the loss was discovered. Generally, the forms did not have a field in which to record such data.

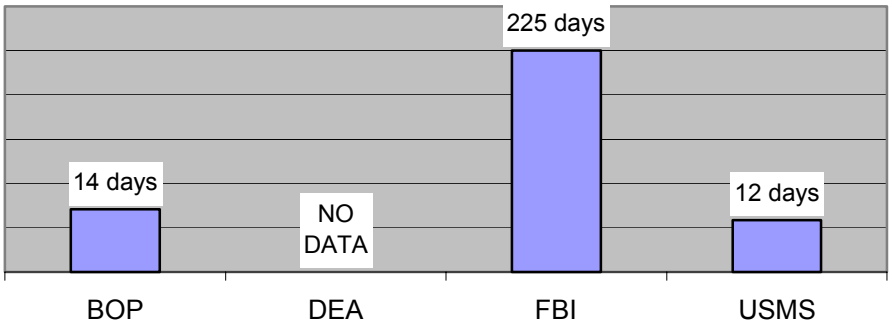
For those cases in which we could determine timeliness, the average reporting times for weapon and laptop computer losses appear in the following graphs.

[34] The stringent controls in place at the BOP, including the fact that equipment is regularly returned to central locations, likely reduced lost items going undiscovered or unreported.

AVERAGE TIME BETWEEN DISCOVERY OF LOSS AND INITIAL WRITTEN REPORT WEAPONS



AVERAGE TIME BETWEEN DISCOVERY OF LOSS AND INITIAL WRITTEN REPORT LAPTOPS



NCIC Records – The National Crime Information Center (NCIC)[35] is generally regarded by law enforcement agencies to be the primary nationwide mechanism for tracking stolen firearms. While the DEA, FBI, INS, and USMS required lost weapons to be entered into NCIC, the BOP did not. The following table displays the differences in policies and practices and the percentage of weapons not entered into NCIC.

[35] NCIC is a nationwide criminal justice information system maintained by the FBI that provides the criminal justice community with immediate access to information on weapons, missing persons, vehicles, license plates, and criminal history records.

COMPONENT REPORTING OF LOST WEAPONS TO NCIC

COMPONENT	POLICY FOR REPORTING LOST WEAPONS	TIMETABLE FOR REPORT	PERCENTAGE OF LOST WEAPONS NOT ENTERED
BOP	NONE	Not Applicable	0%
DEA	YES	Within 48 hours	19
FBI	YES	Immediately	5
INS	YES	As soon as possible	73
USMS	YES	No time requirement	0

DEA officials could not explain why the weapon losses were not entered into NCIC as each had been reported to local law enforcement for entry into the database. In response to our audit at the INS, officials explained that they were in the process of obtaining access to NCIC.

A notable policy at the FBI was to require that all losses of uniquely serialized government property be entered into NCIC, including laptop computers. In our judgment, this policy increases the potential for recovery of this type of sensitive equipment.

Reporting to SEPS – Department regulations[36] require all components to submit a semiannual report to the Department's Security Officer summarizing losses of property that occurred during the previous six months. Each component's Security Programs Manager is required to prepare and submit the reports by January 31 and July 31 for the preceding six-month periods. We reviewed these reports and determined that they were incomplete, untimely, or not submitted. In general, component officials could not fully explain the discrepancies noted.

BOP: Generally, the semiannual reports were timely. However, they did not include 24 of the 27 lost or stolen laptop computers or the 2 missing weapons.

DEA: No reports for 1999 and 2000 were submitted and the first report for 2001 was submitted 36 days late. In addition, the DEA's records included four weapons reported as lost in 2001, but only one appeared on the semiannual report.

FBI: The reports for 2000 and 2001 were submitted from 6 to 106 days late. According to the FBI's inventory records,

[36] DOJ Order 2630.2A, "Protecting and Controlling Federally Controlled Property and Loss/Theft Reporting Procedures."

232 functional weapons, 127 training weapons, and 152 laptop computers were reported lost or stolen during the periods covered by these reports. However, only 9 weapons and 26 laptop computers appeared on the semiannual reports.

USMS: The 2000 and 2001 reports were submitted approximately one month late. Two laptop computers, reported lost in 2000, were not reported to the Department.

In our judgment, these reports were unreliable. Further, the Department was not utilizing them as a means to assess the losses of sensitive property, as discussed on page 29.

Action on Lost and Stolen Weapons and Laptop Computers

According to Department guidelines, all components should establish a Board of Survey or alternative investigative mechanism (Board) to investigate the circumstances surrounding the loss, theft, damage, destruction, and other circumstances adversely affecting personal property. Based upon the recommendations of the Board, component heads are authorized to assess pecuniary liability and dispense disciplinary action.

All components had policies and procedures for referring losses to a Board or alternative investigative unit. We reviewed the referrals to the Boards, the timeliness of the Boards' reviews, and the actions taken as a result of the losses.

Board of Survey Referrals and Reviews – The components did not have consistent policies and practices related to Board referrals and reviews, and many reviews were not timely. Review times ranged from 6 to 588 days after the written loss report.

The USMS policy did not specifically require laptop computer or weapon losses to be referred to the Board for investigation. However, USMS officials stated that, in practice, all weapon losses are referred to the Board. In addition, at the time of our audit, the USMS Board of Survey had not met since November 2000 (16 months); as a result, 50 of the 62 weapon and laptop computer losses had not been adjudicated.

At the FBI, the Office of Professional Responsibility (OPR) provided evidence that only 71 of the 212 lost functional weapons were referred to its office for review.[37] Further, only 10 of the FBI's 317 laptop computer losses

[37] The OPR could not provide us with documentation for the remaining 141 losses; therefore, we were unable to determine if they were ever referred to OPR.

had been referred. Prior to March 9, 2001, FBI policy did not require the routine reporting of lost or stolen laptop computers to the OPR. On March 9, 2001, the Director of the FBI issued a memorandum requiring employees to report all losses of laptop computers to OPR without exception.

INS policy required lost weapons to be reported to its Office of Internal Affairs (OIA) on the first working day after the loss. Between January 1, 1996, and September 30, 1999, the OIA received 45 referrals, while a total of 74 weapon losses were entered into NCIC.

The DEA required weapons-related property losses to be referred to its Board of Professional Conduct for investigation. We found that 15 of the 16 weapon losses had been referred and reviewed; the Board's decisions were rendered 61 to 431 days from the date of loss. The remaining instance involved an employee who had left the DEA and, as a result, the Board made no recommendation.

The BOP required all weapons and laptop computer losses to be referred to its Board for review. All losses were referred and reviewed and review times ranged from 6 to 588 days.

Management Action – After the Boards have completed their reviews, component heads are responsible for acting on the findings and recommendations. This can include assessing financial liability, pursuing collection, and implementing disciplinary action.

In total, we found evidence that only 15 of the 400 laptop computer losses (4 percent) and 41 of the 236[38] weapon losses (17 percent) have so far resulted in recommendations for disciplinary action. These low percentages are primarily attributable to the fact that, as noted above, many losses have not been referred to or reviewed by the Boards. In our judgment, these numbers could suggest to employees that the components are not taking the loss of these items seriously and that there is a good chance that no action will be taken on sensitive property losses.

For those instances in which the Boards have completed their reviews, the percentage of cases in which disciplinary action was recommended is significantly higher. At the DEA, 10 of the 15 weapon losses (66 percent) reviewed by the Board resulted in disciplinary actions, including letters of reprimand and recommendations for suspensions without pay. At the FBI, 37 of 70 (53 percent) completed reviews of weapon and laptop computer

[38] We did not include the 539 INS weapons losses in this number because our earlier INS audit did not examine disciplinary action for weapons losses.

losses resulted in disciplinary action; 11 investigations were pending at the time of our audit. Disciplinary actions included letters of censure and recommendations for suspensions without pay. Following review by the Board at the USMS, 9 of 12 weapon and laptop computer losses (75 percent) resulted in advisory letters to the responsible offices. The BOP did not execute any disciplinary action for the 29 weapon and laptop computer losses reviewed.

Return of Equipment from Separated Employees

Department guidelines[39] stipulate that components must have effective procedures to provide assurance that assets do not leave the possession of the government. However, the components' procedures were not effective,[40] and property assigned to departed employees was unaccounted for. For example, in June 2001, the FBI's Firearms Training Unit found that 31 weapons of separated agents could not be accounted for. About one month later, two FBI weapons were recovered at the scene of an accidental shooting. These weapons had been assigned to an agent who died in April 2001 and the FBI had not taken the appropriate steps to retrieve the firearms. In addition, we noted that the BOP, DEA, and INS also experienced problems regarding the return of property by separated employees.

The components must strengthen their procedures for retrieving and documenting the return of sensitive property from separated employees. This is an area in which controls can be strengthened and losses can be significantly minimized.

Disposal of Sensitive Property

Department regulations[41] state that information technology systems that have processed, stored, or transmitted sensitive but unclassified and/or classified information shall not be released from a component's control until the equipment is sanitized and all stored information has been cleared. We tested laptop computer disposals at the components and found that the majority of the records at the BOP and the FBI did not specify the contents

---

[39] DOJ Order 2110.41, "Clearance Procedures for Employees Separating from or Reassigned within the Department of Justice."

[40] The BOP did not have uniform guidance or a checklist for separated employees to ensure that all property had been returned. At the DEA, FBI, INS, and USMS, we noted problems with the components' established checklists including: lack of relevant accountable signatures, failure to enforce the use of the form, and failure to include information regarding weapons.

[41] DOJ Order 2640.2D, "Information Technology Security."

of the machines or contain a certification that all sensitive information had been removed. We believe that it is essential that this step be taken and documented to ensure that all sensitive information has been protected and that the public is not harmed through the disclosure of sensitive information.

IV. WEAK DEPARTMENT PROPERTY MANAGEMENT OVERSIGHT CONTRIBUTED TO THE DEFICIENCIES AT THE COMPONENTS

The Department has not taken an active role in the management of property at the components. Instead, it has established and promulgated broad guidelines and delegated responsibility to the component heads. As a result, the Department has been unaware of significant losses of sensitive property and related control concerns.

Criteria

The Justice Management Division (JMD), headed by the Assistant Attorney General for Administration, is responsible for planning, directing, administering, and monitoring compliance with Department-wide policies, procedures, and regulations concerning property.[42] General property management guidelines for federal agencies are prescribed by the Federal Property Management Regulations.[43] The Department has implemented and supplemented these regulations with the Justice Property Management Regulations (JPMR).[44] The JPMR govern the acquisition, utilization, management, and disposal of personal and real property and are issued to establish uniform property management policies, regulations, and procedures in the Department.

Justice Property Management Regulations

As established by the Assistant Attorney General for Administration, the components are fully vested with the responsibility to manage their property resources. The Department has maintained little control over their activities, and the JPMR does not establish a system for the JMD to oversee property management within the components.

According to the JPMR, bureau heads[45] are delegated to designate a Property Management Officer (PMO) responsible for ensuring compliance

---

[42] Code of Federal Regulations, Title 28 "Judicial Administration," Chapter 1 "Department of Justice," Part 0 "Organization of the Department of Justice."

[43] Code of Federal Regulations, Title 41 "Public Contracts and Property Management," Chapter 101 "Federal Property Management Regulations."

[44] DOJ Order 2400.3.

[45] In addition to the BOP, DEA, FBI, INS, and USMS, the JPMR includes the following in its definition of "bureaus": the Office of Justice Programs; Federal Prison Industries, Incorporated; the OIG; and the JMD Facilities and Administrative Services Staff.

with internal and Government-wide authorities and guidelines to determine source, acquisition, receipt, accountability, distribution, and disposal of property. Further, the bureau heads are responsible for:

- issuing detailed operating procedures to protect against fraud, waste, and abuse of federal property and advising managers and employees of their responsibilities with respect to federal property;
- ensuring care and security of property, to include storage, handling, preservation, and preventive maintenance;
- creating and maintaining complete, accurate inventory control and accountability records;
- planning and scheduling property requirements to assure that equipment is readily available to satisfy program needs while minimizing operating costs and inventory levels; and
- maximizing utilization of available property for official purposes.

The JPMR requires the bureaus to provide a copy of their manuals, operating guides, and detailed procedures to the JMD. However, the JPMR does not stipulate that JMD must review these documents or oversee any of the bureaus' other responsibilities.

JMD Facilities and Administrative Services Staff, Property Management Services

Within the JMD, property management is delegated to the Facilities and Administrative Services Staff, Property Management Services office (JMD Property Office). This office administers the JPMR and provides property management services to offices, boards, and divisions of the Department. These services include, but are not limited to, maintaining the official property records, initiating physical inventories, and assisting in the disposal of property.

For the bureaus, JMD Property Office personnel act in an advisory role. They promulgate guidance and request ad-hoc information regarding physical inventories, inventory levels, and responsible personnel. According to JMD Property Office personnel, they do not have explicit authority to monitor the bureaus, but they recognize a need for obtaining information from them. Without stated authority, bureau compliance is not assured. In its advisory role, the office performs the following activities:

Quarterly PMO Meetings – According to the JMD Property Office, it holds quarterly meetings with designated PMOs as a forum to provide information on program initiatives and exchange ideas and strategies. At these meetings, the JMD Property Office provides information on new or pending legislation, emerging technology, new theories for resolution of common issues, and internal and external training opportunities. The meetings are also used as a central place to identify and correct any problems and to obtain concurrence on proposed Department-wide policies, procedures, and technologies.

At the July 2001 and March 2002 meetings, JMD presented a proposal for the use of advanced technology to manage property in the Department. The technology includes the ability to track the location of property using computer software, radio frequency tags, and global positioning systems. The use of such technology could significantly help the Department locate missing property. Also, recent meetings have been used to discuss the JFMIP guidelines and integration/reconciliation of accounting and property systems.

Uniform Training – JMD has proposed to the bureaus that they seek to obtain training from the National Property Managers Association (NPMA). The NPMA offers studies in government property management and certification at three different levels: a certified professional property specialist, a certified professional property administrator, and a certified property manager. To maintain the current level of certification or seek the next level of certification, the NPMA requires individuals to pass, with 75 percent proficiency, a series of comprehensive tests and essays regarding personal property management.

According to the JMD Property Office, all of the components have acquired NPMA certification for key individuals. Although the NPMA is the recognized leader in developing property management standards and proficiencies for industry, universities, and government, the Department is one of few federal agencies that has trained and certified its property management professionals.

Information Requests – At various times, the JMD Property Office has requested the bureaus to provide property management information. For example, in June 2001, the components were requested to provide confirmation that their Board of Survey procedures were in compliance with the JPMR. In addition, the bureaus were asked to provide an evaluation of their property management activities for Fiscal Years 2000 and 2001. These evaluations included the following areas:

- identification of the property management system software, users, centralization level, and date of last upgrade;

- proposed modifications if the automated system did not meet the JFMIP integration requirements;

- the number and dollar value of property recorded on inventory and the number of transactions processed;

- detailed information regarding property dispositions (such as excessed, transferred, destroyed, donated, and sold property); and

- the date of the last physical inventory, including the number of inventories received and the number of inventories completed.

In response to the above request, the FBI informed the JMD that a physical inventory was performed between February 1999 and February 2001. The submission noted that the inventory was not complete. However, the FBI did not fully disclose that the last completed inventory was before 1993.

As a result of our audits, the JMD Property Office also initiated monitoring of the bureaus' weapon and laptop computer inventory, including reported property losses. In February 2002, the bureaus were requested to provide to the JMD the following information on a quarterly basis:

- the total number of such items in inventory;

- the number of items lost, missing, or stolen; and

- a summary of the bureaus' efforts to: (1) account for the missing items, (2) identify laptop computers that may have contained classified information, and (3) ensure strict accountability of these items.

As illustrated by the above requests, the JMD Property Office has not taken a strictly hands-off approach to property management in the bureaus. However, since the efforts have been advisory in nature, no action has been taken to verify the information provided by the bureaus. With added authority, the JMD Property Office could be tasked with gathering information at regular intervals and ensuring bureau compliance.

JMD SEPS

Although it has primary responsibility, the JMD Property Office is not the only JMD office with duties related to the control and accountability of weapons and laptop computers. Some specific tasks are undertaken by the SEPS office, headed by the Department Security Officer. Two SEPS offices are involved: the Information and Technical Security Group and the Facilities and Personnel Protection Group. Their tasks include controlling information technology resources used to store and process sensitive and classified information and receiving semiannual reports of property losses.

Information and Technical Security Group – As noted on page 11, SEPS maintains records of the number of computers, including laptops, that have been authorized for processing classified information within the Department. Along with this task, the SEPS Information and Technical Security Group establishes policy for the security of these machines and the sensitive data they process.

In July 2001, the Department strengthened the requirement that components report incidents of security violations, such as the loss of computers authorized to process classified information. According to the new regulation,[46] Department components must report any incident involving the loss, compromise, or other event affecting the security of a classified system *immediately*. Before this regulation was put into effect, components were to report security violations within 10 working days. Further, components are now required to provide a detailed account of the loss, corrective actions taken to contain the incident, and measures taken to prevent a similar occurrence.

Facilities and Personnel Protection Group – The SEPS Facilities and Personnel Protection Group (Protection Group) is currently the repository of the required Department Semiannual Theft Reports noted on page 20. According to officials in this group, these reports are reviewed to gain perspective of the extent of losses of Department property. The primary concerns had been the economic impact of the losses and any trends that implied a physical security problem in a specific location, but little to no attention was paid to the sensitivity of the lost property or the corrective actions taken by the components to address the situation and to reduce future losses.

It appears that in its present form, the reporting requirement does not assist the Department in assessing the impact of sensitive property losses.

---

[46] DOJ Order 2640.2D, "Information Technology Security."

Further, as previously noted, we found the components' compliance with the requirement to be generally inadequate because reports were incomplete, inaccurate, or not submitted.

We discussed the Department Semiannual Reports with both the Protection Group and the JMD Property Office. Protection Group officials acknowledged the office is not reviewing the entirety of the information and that the reports could be used in a much more analytical fashion. Similarly, Property Office personnel recognized that the responsibility was not entrusted to the proper operating unit and that the regulation needed revision. We suggested the requirement be continued but that it be incorporated into the JPMR and that the Property Office be given responsibility for ensuring component compliance.

V. OIG CONCLUSIONS AND RECOMMENDATIONS

In our judgment, it is critically important for the Department to increase its role in the management of sensitive property such as weapons and laptop computers. Loss of this property can result in danger to the public or compromise national security or law enforcement investigations. We believe it is an opportune time for the Department to take action to tighten controls that are currently weak, inadequate, or not fully implemented.

At the conclusion of our audits at the individual components, we made specific recommendations for improvement to the component heads. These recommendations were detailed in our individual reports and are not repeated here. Generally, our recommendations have been well received and corrective actions are underway. Based on the weaknesses we saw at the Department and component level we offer several general recommendations to strengthen controls over weapons and laptop computers.

The Department Should Review the Components' Ratios of Weapons to Employees

The components' ratios of weapons to agent/officer varied from less than one to over four. The component average was about 2 weapons per employee. We recognize that the needs of the components differ; however, we suggest that the Department consult with the component heads to assess the actual needs and determine if a Department guideline should be established.

1. *We recommend that the Assistant Attorney General for Administration, in consultation with the component heads, review the ratios of weapons to agent/officer and determine if the ratios are appropriate and if a Department guideline should be established.*

The Department Has Not Implemented the JFMIP Guidance on the Integration of Accounting and Property Systems

None of the components' accounting and property systems are integrated or reconciled for non-capitalized controlled personal property (including weapons and laptop computers). As a result, we identified purchased property that was not added to the inventory records. JFMIP guidance calls for this integration to facilitate reconciliation between systems and improve data accuracy. Integration or reconciliation would help ensure

that transactions for property purchases entered into the accounting system result in the addition of property to the inventory management system.

The JMD Property Office has brought the JFMIP guidance to the components' attention. However, although the Justice Property Management Regulations (JPMR), which govern property management in the Department, require the components to maintain complete and accurate inventory records, they do not specify that the accounting and property systems should be integrated or reconciled.

2. *We recommend that the Assistant Attorney General for Administration revise the JPMR to include the requirement for integration or reconciliation of accounting and property systems.*

Lack of Department Restriction Resulted in Weak Weapon Purchase Controls at the BOP

The BOP allowed institutions and local offices to purchase weapons using credit cards. We recommended that the Director of the BOP prohibit the use of credit cards to purchase weapons as a means to further control its weapon inventory and the BOP has initiated corrective action. This additional control is warranted because weapons are possibly the most highly sensitive type of property due to their lethal nature. We discussed this issue with Department officials, who agreed that the use of credit cards to purchase weapons at the local level should be prohibited.

3. *We recommend that the Assistant Attorney General for Administration revise Department level credit card directives to prohibit the purchase of weapons at the local level.*

Inconsistent Policies for Securing Weapons and Laptop Computers Resulted in Avoidable Losses of Property

The JPMR and other Department regulations do not prescribe minimum standards for weapon storage. At the DEA, the component with the most stringent policy for securing weapons outside component space, 25 percent of weapon losses occurred because the responsible employees violated component policies and stored their weapons in unattended vehicles. Conversely, at both the FBI and USMS, which allowed handgun storage in unattended vehicles to some degree, the percentage of weapon losses from unattended vehicles was significantly higher. At the FBI, 44 percent of functional weapon losses for which there was an explanation occurred because they were left in unattended vehicles. Up to 50 percent of weapon losses at the USMS was attributed to storage in vehicles.

4. *We recommend that the Assistant Attorney General for Administration, in consultation with the component heads, establish and implement a standard policy for the security and storage of weapons outside Department facilities, particularly in vehicles.*

The Department Should Revise the Definition of Controlled Personal Property to Ensure that all Weapons and Computers are Included

The INS and USMS both had types of sensitive property that were not within the definition of controlled personal property. At the time of our audit, the INS's definition of controlled property excluded property costing $1,000 or less, including those items with data storage capability such as laptop computers. The USMS maintained a supply of stun guns and stun belts that were not designated as controlled personal property. In our judgment, the Department should ensure that these types of property are classified as controlled personal property throughout the components. In doing so, the Department will ensure that these items are subject to physical inventory and inclusion in the official property management records, thereby reducing the susceptibility for loss.

5. *We recommend that the Assistant Attorney General for Administration revise the controlled personal property definition to include weapons of all types and all items with data storage capability.*

Lack of Component Commitment and Department Oversight Resulted in Failure to Complete Physical Inventories

At the initiation of our audit in August 2001, the FBI had failed to complete an inventory since before 1993. Although Department and internal FBI guidelines required biennial inventories of controlled personal property, the FBI did not comply. It is simply not acceptable for the FBI to have failed to complete a physical inventory of controlled personal property in almost ten years and for the Department to be unaware of this weakness. Further, the failure of the FBI to complete an inventory no doubt led to many of the FBI's problems related to the accountability of weapons and laptop computers discussed in this report.

The JMD Property Office requested information regarding the conduct of physical inventories, but the FBI did not disclose the fact that complete inventories were not up to date. The JPMR does not require the JMD Property Office to monitor the completion of physical inventories nor does it authorize the JMD to verify that an inventory has been conducted.

6. *We recommend that the Assistant Attorney General for Administration require components to report their physical inventory activities to the JMD Property Office. Further, the Property Office should be authorized to monitor the submissions and take necessary steps to verify accuracy*.

The Department Should Consider Revising the Physical Inventory Requirements for Weapons

The BOP, DEA, INS, and USMS required weapons to be physically inventoried annually; the FBI did not. As the FBI incurred substantial losses of weapons, it is prudent to strengthen the Department guidelines to require weapons to undergo physical inventory annually.

7. *We recommend that the Assistant Attorney General for Administration revise physical inventory guidelines to include a requirement that weapons be inventoried at least annually.*

The Department Should Continue to Encourage the Components' Use of Advanced Technology

Unfortunately, the components were not taking advantage of technological advances in the area of property management. The components were making only minimal use of barcodes and scanning devises to assist in the conduct of physical inventories. The FBI was the only component to make widespread use of barcode scanners; however, officials attributed many physical inventory delays to technological problems encountered with the barcode equipment.

Recently, the Department has researched the possibility of using software, radio frequency tags, and global positioning systems to track property and reduce losses. In our judgment, the Department should continue to pursue these avenues and support component initiatives to implement other advanced technologies.

In addition, we found that the USMS was utilizing a unique scheduling system for its physical inventories. Specifically, it conducted its inventories on a continual basis, ensuring that the entire USMS is not undergoing its controlled personal property physical inventory at the same time. Thus, headquarters work remains at a more consistent level, which can minimize inaccuracies and reduce the likelihood of other property management tasks being neglected.

8. *We recommend that the Assistant Attorney General for Administration encourage the components to use advanced technologies in managing property. Further, the Department should explore the USMS scheduling method to determine if more widespread use of the USMS's system throughout the Department would improve property management.*

Weak Policies Regarding Loss Reports within the Components

The JPMR, which is the governing criteria for property management, and other Department guidelines are silent on several issues regarding the reporting of property losses within the components. Establishing consistent minimum standards will help ensure that adequate information is gathered at the most opportune time, that is, immediately following the discovery of a loss when the potential for recovery is at its highest. This is particularly important in that the public can be harmed by the loss of sensitive property.

Our reviews revealed the following weaknesses in the policies and procedures at the components that could be remedied, in part, through the establishment of minimum Department standards:

- Neither the BOP nor the FBI had a time requirement to submit the initial loss report. For weapons, the average amount of time between loss and the resulting report at the FBI was over 4 years.

- Loss reports did not consistently require the inclusion of the sensitivity of information stored on lost laptop computers.

- Loss report forms did not consistently require the date the loss was discovered. As a result, we were unable to gauge the timeliness of many reports.

- The BOP did not have a policy for reporting weapon losses to NCIC, and the policies related to the timing of NCIC reports at the remaining four components were inconsistent.

- Only the FBI required laptop computer losses to be reported to NCIC, which has the capability of storing information on lost property. Reporting laptop computers to NCIC increases the potential for recovery of Department equipment.

9. *We recommend that the Assistant Attorney General for Administration, in consultation with the component heads, establish and implement*

minimum standards for the reporting of lost weapons and laptop computers within the components. The revised policies should address: (1) the timing of the initial loss report, (2) the inclusion of the loss discovery date and the sensitivity of information stored on lost laptop computers, and (3) reporting weapon and laptop computer losses to NCIC and the timing of such reports.

Ineffectual Policy Regarding Loss Reports to the Department

The Department requires the components to report property losses to the SEPS Facilities and Personnel Protection Group semiannually. However, the components have not fully complied with this regulation and the reports were inaccurate, incomplete, or not submitted. Further, the Department is not fully utilizing the reports to understand and act on the losses. Moreover, prior to our audit, the Department did not monitor the components' initiatives to reduce losses of weapons and laptop computers.

10. *We recommend that the Assistant Attorney General for Administration revisit the Department policy for reporting property losses. This should include transferring review responsibility to the JMD Property Office, along with the authority to monitor component submissions for compliance and corrective initiatives.*

Weaknesses in Department Policy for Referrals to and Reviews by Boards of Survey Resulted in Untimely Reviews or Lack of Referral

Department regulations require Boards of Survey to conduct "prompt" investigations into the circumstances that caused property losses. The timing of Board of Survey reviews ranged from 6 to 588 days after the losses were discovered. It is critical that Board of Survey reviews take place as soon as practicable upon the discovery of the loss. Conducting these reviews almost two years after a loss is reported is unacceptable.

In addition, while Department regulations require certain property losses to be referred to Boards of Survey, they do not specify that losses of any particular types of sensitive property, including weapons and laptop computers, must be referred for investigation.

11. *We recommend that the Assistant Attorney General for Administration revise the Department policy related to Boards of Survey to ensure that all weapon and laptop computer losses (along with any other types of sensitive property) are referred to the Board for review. Further, the Department should establish a time standard for the initiation of the Board of Survey review.*

Weak Department Policy and Ineffective Component Procedures Resulted in Property Not Retrieved from Separated Employees

Department guidelines stipulate that components must have effective procedures to provide assurance that assets do not leave the possession of the government. The guidelines dictate that component heads develop and distribute an accountable item checklist designed to fit the needs of the organization. However, our audits revealed that the components' procedures were not effective to ensure that sensitive property, such as weapons and laptop computers, was retrieved from separated employees. In fact, in 2001, the FBI found that at least 31 weapons of separated agents could not be accounted for or had not been retrieved. The BOP, DEA, and INS also experienced problems regarding the return of property.

The effectiveness of the components' procedures could be improved if the Department established minimum standards for inclusion in the required checklists for separated employees. The Department must recognize the difference among types of property and enact more specific and stringent policies for sensitive property such as weapons and laptop computers.

12. *We recommend that the Assistant Attorney General for Administration require checklists for separating employees to specifically include sensitive property such as weapons and laptop computers and approval by responsible personnel, such as property and firearms custodians.*

Department Policy for Disposal of Laptop Computers Does Not Specify that the Removal of Sensitive Information Needs to be Documented

Although Department regulations require components to fully remove stored information from computer equipment before disposing of the machine, the regulation does not specify that the disposal documents include information about the removal. Protecting sensitive information and documenting the steps taken are important to ensure that the public and law enforcement activities are not harmed through improper disclosure. Our testing of laptop computer disposals at the components disclosed that the majority of the records at the BOP and the FBI did not address the removal of sensitive information.

13. *We recommend that the Assistant Attorney General for Administration revise the regulations to ensure that steps to remove information from laptop computers are adequately documented.*