U.S. Department of the Interior
Office of Inspector General

Evaluation of the Department of the Interior's Accountability of Desktop and Laptop Computers and their Sensitive Data

Report No. WR-EV-MOI-0006-2008

April 2009

Description of Cover Graphics:

- Computer port and tower courtesy of FreePhotosBank.com
- Laptop courtesy of Yankodesign.com
- Laptop keyboard and key courtesy of Securitywatch.co.uk

United States Department of the Interior

Office of Inspector General
Western Region
Federal Building
2800 Cottage Way, Suite E-2712
Sacramento, California 95825

April 24, 2009

Memorandum

To: Debra E. Sonderman
Director, Office of Acquisition and Property Management

Sanjeev Bhagowalia
Chief Information Officer

From: Michael P. Colombo
Regional Manager

Subject: Final Report - *Evaluation of the Department of the Interior's Accountability of Desktop and Laptop Computers and their Sensitive Data*
(Report No WR-EV-MOI-0006-2008)

The results of our evaluation found that the Department of the Interior (Department), as a whole, could not account for the computers purchased, as there is no uniform policy for the tracking and chain of custody of portable computer equipment. Instead, bureaus independently decide what, if any, property controls to put in place. Our objective was to evaluate the Department's physical controls over desktop and laptop computers to ensure these devices, and the information stored on them, are protected from loss and misuse. Our testing and validation of computer property revealed that 13 computers were missing and that nearly 20 percent of more than 2,500 computers sampled could not be specifically located. Compounded by the Department's lack of computer accountability, its absence of encryption requirements leaves the Department vulnerable to sensitive and personally identifiable information being lost, stolen, or misused.

Given the Department's diverse missions, varying and often opposing constituencies, and controversial issues including environmental and Indian trust matters, infrastructure assets such as dams, bridges, and monuments, and land and minerals management activities, information control is essential. An example of the consequence for failure to maintain this control can be demonstrated by the recent theft of two laptops in a Nashville, Tennessee government office that contained the names and Social Security numbers of the county's 337,000 registered voters. As a result, the county government purchased identity-theft protection expected to cost about $1 million to mitigate the potential damage to voters from the theft.

To address the computer information vulnerability discussed above, we recommend that the Department, (1) establish a uniform Department-wide system-controlled chain of custody property system for computers, (2) incorporate information sanitization procedures in conjunction with property disposal procedures, (3) require that the loss or theft of all computers be reported to the Department's Computer Incident Response Center, and (4) take immediate steps to encrypt all portable computers throughout the Department. (See Appendix 1 for the objective, scope, methodology, and other related coverage of our evaluation and Appendix 2 for sites visited or contacted.)

We ask that you apprise us within 30 days of the actions you take or plan to take in response to this report. We appreciate the cooperation shown by the Department bureaus and offices during our review. If you have any questions regarding the report, please call me at (916) 978-5653.

cc: Assistant Secretary for Policy, Management and Budget
Associate Director, Finance Policy & Operations

Contents

Acronyms and Other Reference Terms

BIA ..... Bureau of Indian Affairs
BLM ..... Bureau of Land Management
BOR ..... Bureau of Reclamation
CIRC ..... Computer Incident Response Center
Department ..... Department of the Interior
FWS ..... Fish and Wildlife Service
GAO ..... Government Accountability Office
GSA ..... General Services Administration
IHS ..... Indian Health Service
ISD ..... Information Security Division
IT ..... Information Technology
MMS ..... Minerals Management Service
NBC ..... National Business Center
NPFR ..... Notification of Potential Findings and Recommendations
NPS ..... National Park Service
OIG ..... Office of Inspector General
OMB ..... Office of Management and Budget
OSM ..... Office of Surface Mining
USGS ..... U.S. Geological Survey

Accountability Requirements for Desktop and Laptop Computers

In recent years, significant control weaknesses over computer equipment and incidents of lost or compromised sensitive personal information have been found within various federal agencies. (See Appendix 1 for examples of other reports.) The risks associated with loss of sensitive information spurred the Congressional Committee on Government Reform to open a query in 2006 to determine the magnitude of potential data loss across the government. The Committee determined that data loss is a government-wide occurrence and found that all 19 agencies queried, including the Department of the Interior, reported data loss. Additionally, the Committee found that agencies do not always know what has been lost, thus physical security of data is essential.

In May 2006, the Department of Veterans Affairs (VA) announced that computer equipment containing the personal information of approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee.

-- U.S. House of Representatives Committee on Government Reform

The lack of accountability for desktop and laptop computers should be of great concern to the Department and its eight bureaus. The Department is a large, decentralized agency with diverse missions and numerous offices across the U.S., Puerto Rico, U.S. territories, and freely associated states. With nearly 70,000 employees using portable computers to help further their efforts to meet the Department's mission of resource protection, recreation management, scientific research, and community service, the necessity of addressing concerns about the Department's accountability for these numerous desktop and laptop computers located across the nation should come as no surprise.

In 2002, the Federal Information Security Management Act was enacted to provide a comprehensive framework for ensuring the effectiveness of security controls over information and information systems to prevent unauthorized access, use, disclosure, disruption, modification, or destruction to ensure the integrity, confidentiality, and availability of such information. The Department also has policy that provides for an information technology (IT) security program that must include minimum, adequate, and appropriate levels of protection for all IT resources within the organization, including hardware, software, and physical and environmental facilities that support information systems. This policy further stipulates that laptop computers, personal data assistants, and other portable computing devices not be left unattended, in plain view, in unattended vehicles, hotel rooms, or uncontrolled offices.

Researchers at Credant Technologies have determined that 25% of laptops are stolen from the office or the owner's car. Another 14% are lost in airports or on airplanes.

-- ASIS International Foundation

Despite these policies, the Department does not currently require that desktop and laptop computers be tracked and controlled in a property management system. While Interior Property Management Directives require that personal property with an acquisition cost of at least $5,000 or classified as sensitive be recorded in a property management system, desktop and laptop computers do not generally meet these thresholds. The Department defines sensitive property as that which is system-controlled, regardless of value, by detailed accountability records, and at a

minimum must include firearms and museum property. The National Business Center (NBC) recently began tracking laptop computers for the Department. However, NBC is facing challenges in doing so as it relies on individual Departmental offices to notify it of laptop computer purchases.

Custody of Desktop and Laptop Computers Not Readily Known

We found that the Department, as a whole, does not readily know where or to whom its desktop and laptop computers are assigned. The Department and its bureaus' ability to produce complete and accurate inventory records is varied[1]; two bureaus (BLM and OSM) provided good records, two bureaus (MMS and NPS) provided average records, the Department and one bureau (FWS) provided poor records, and three bureaus (BIA, BOR, and USGS) did not provide any inventory records. This lack of accountability stems from the Department not requiring that computers be treated as sensitive property. This designation of sensitive property is critical, as computers do not commonly meet the accountability threshold and thus are not formally tracked. While bureaus are allowed to make such a designation themselves, they are not held responsible for how they implement their own guidance. For example, despite Fish and Wildlife Service's sensitive designation of its laptop computers, it was unable to provide basic physical location information for 450 of the 473 computers (or more than 95 percent) sampled. Within the Department, five bureaus have chosen to classify laptop computers as sensitive and three have not, as depicted in Table 1.

Table 1: Classification of Laptops and Quality of Inventory Records

Bureau	Sensitive	Records
Bureau of Land Management (BLM)	Yes	Good
Office of Surface Mining (OSM)	Yes	Good
Minerals Management Service (MMS)	Yes	Average
National Park Service (NPS)	Yes	Average
Department	No	Poor
Fish and Wildlife Service (FWS)	Yes	Poor
Bureau of Indian Affairs (BIA)	No	None
Bureau of Reclamation (BOR)	No	None
U.S. Geological Survey (USGS)	No	None

Given the Department's inability to provide complete property and location information, we were unable to establish a computer equipment universe and limited our physical testing to the Sacramento area. To supplement this data, we requested sales information from Dell, the Department's primary provider of IT equipment. This raw sales data allowed us to compile an inventory of computers that the Department should be accountable for and randomly sample 20 percent of the computers (See Table 2 for details).

[1] We determined good inventory records to be those that contained complete location and employee custodial information for desktop and laptop computers, average inventory records to be those that had some complete information only after additional time and effort, and poor inventory records to be those that lacked complete information even after additional efforts were made to obtain the information.

We presented this sample to the various bureaus with the expectation of receiving specific location and custodial information. However, of the 2,503 computers tested, 462 computers (or nearly 20 percent) were not located (Table 2). Because the Bureau of Reclamation and the Fish and Wildlife Service did not adequately identify the location of their laptop computers within a specified timeframe, we issued notices of potential findings and recommendations (NPFRs) in December 2008 to both agencies. In response to our NPFRs, the Bureau of Reclamation performed additional work and identified the location of its computers. Of the 462 computers that were identified as "not located," 13 were identified as missing (BOR-10, Department-2, and FWS-1) during the inventory process. Eight of these computers were identified as lost or stolen, with one having been reported to the Department's Computer Incident Response Center (CIRC). Interestingly, these 13 computers would not have been identified as lost, stolen, or missing if not for our inventory testing because of the Department's poor accountability for its computers.

Table 2: Computer Testing Results

Bureau	Sampled	Not Located
BLM	337	0
OSM	24	0
MMS	79	0
NPS	559	0
Department	97	2
FWS	473	450
BIA	223	0
BOR	216	10
USGS	495	0
Summary	2,503	462 *(19 percent)*

Disposal Process Not Adequate

At the bureaus and offices visited or tested, we generally found the documentation for disposal of desktop and laptop computers to be inadequate. At some of the office locations visited, we could not determine if a particular computer had been disposed of. For example, at BOR's Mid-Pacific Regional Office computers were batched in large quantities for disposal with no service tag or serial numbers to tie into the supporting documentation and at FWS' California State Office some of the computers we tested had no documentation to support that the disposal occurred. Additionally, while there are General Services Administration (GSA) regulations and Departmental policy for computer disposal, there were varying methods of documenting that disposed computers were properly sanitized (all memory devices erased).

GSA defines "sensitive personal property" to include all items, regardless of value, that require special control and accountability due to unusual rates of loss, theft or misuse or national security considerations, such as information technology equipment with memory capability (emphasis added).

GSA regulations establish the disposal order of personal property, and require that agencies implement policies and procedures to remove sensitive or classified information from property prior to disposal. The Department's policy addressing personal property disposal considers virtually all computers to potentially contain sensitive information. Therefore, bureaus and offices are to remove sensitive data when transferring, donating, or disposing of computer equipment using the appropriate physical or electronic sanitization methods given the level of sensitive information stored on the computer.

We found that the all bureaus had policies or procedures to either dismantle and destroy or sanitize computer equipment; however, compliance with them varied widely. The methods

used to demonstrate that computers were properly sanitized ranged from internal disposal forms with IT certification statements to labels placed on the equipment to IT Helpdesk logbooks. Although we did not physically determine if computers were sanitized, we concluded that the documentation process for recording this activity needs to be improved, standardized, and controlled to ensure the integrity of the sanitization process.

Incidents of Loss and the Lack of Encryption

During October 2007 through November 2008, the Department and its bureaus reported 66 incidents of laptop loss to the Department's CIRC. (See Table 3 for details.) Except for the Office of Surface Mining, who saw no loss during this period, the Department and each of its bureaus reported a minimum of two incidents of laptop loss. Incidents, which may have included more than one laptop, are classified as low, medium, or high criticality. Interestingly, while the U.S. Geological Survey, Bureau of Land Management, and National Park Service saw the highest total incidents of loss, they were also the agencies that were able to most readily identify and provide accurate laptop information to us, whether through inventory or other records, when compared to their counterparts.

Table 3: Incidents of Laptop Loss by Criticality

As reported to CIRC during October 2007 through November 2008.

Bureau	High	Medium	Low	Total
USGS	5	17	3	25
BLM	3	7	1	11
NPS	4	6		10
FWS	3	4		7
BOR		5		5
MMS		3		3
Department	2	1		3
BIA		1	1	2
Summary	**17**	**44**	**5**	**66**

While we found that the Department and bureaus reported incidents of loss to CIRC, it is only a Departmental requirement to report missing property with a value of $5,000 or more and all sensitive property. Instead, bureaus generally use internal reports of survey to identify missing computers.

The potential for misuse of stolen or lost information further exposes the Department and its bureaus, as we found that desktop and laptop computers are generally not encrypted. The Office of Management and Budget (OMB) issued a memorandum in 2006, requiring encryption of all data on mobile devices, such as laptop computers. Our Information Security Division (ISD) found very limited implementation of a solution addressing OMB encryption requirements.

Organizations today must be able to locate and report on the activities of computers that have been used for unauthorized activities, gone missing or have "drifted" within an organization.

-- Information Systems Control Journal

During the past year, ISD conducted fieldwork at six bureaus in order to gain a better understanding of their handling of sensitive information and associated safeguards. We found similar vulnerabilities across all bureaus. Specifically, we found non-compliance with federal and Departmental IT security requirements, as well as inadequate physical security in many locations.

Bureaus have implemented some security procedures and are in the process of evaluating their implementation of government-wide security requirements; however, we determined that the safeguards surrounding the protection of sensitive information are inadequate. Specifically we identified the following weaknesses, which adversely impact the bureaus' ability to protect sensitive information:

- **Physical security** – With the exception of NBC, ISD gained unauthorized physical access to at least one facility at each bureau evaluated and successfully accessed IT resources. Physical access to such resources allowed us to circumvent normal access controls, exploit configuration vulnerabilities, and gain administrative access to workstations on the network. For example, ISD gained unauthorized access to a data center at MMS when a secondary door was found unsecured. In many other locations, our personnel routinely gained unauthorized access by following authorized personnel when they opened a door. Once inside, our staff freely moved between offices and cubicles. In four remote office facilities, our staff simply walked in the front door and gained access to bureau assets, documents, and IT resources unchallenged. In those same four facilities, we departed at our leisure without being challenged.

- **Incident response** – Procedures covered electronic data but not paper documents.

- **Continuous monitoring –** Bureaus had not fully implemented their IT system monitoring tools and capabilities, thus access to sensitive electronic documents went undetected and unreported.

- **Safeguards surrounding portable devices** – Bureaus were unable to control the use of personally-owned or government-furnished portable storage devices (USB drives, external portable hard drives, laptops) thus they have limited control over their data. We found very limited implementation of a solution addressing the requirements of the OMB M-06-16, 'Protection of Sensitive Agency Information.' Some bureaus had implemented encryption solutions for laptops, although as of the date of ISD's evaluations, there was no enterprise solution for cryptographic protection of laptops. A small number of key personnel had an encryption solution on their laptops, but the majority of laptops were not encrypted.

In our discussions with bureau officials, this condition was attributed to a Departmental moratorium on the purchase of encryption solutions until the establishment of an official DOI-approved solution. The Department selected and approved an encryption product at the end of October 2008; however, implementation has not occurred and timelines for implementation will be established by each bureau.

The Department's poor computer accountability, uncertainty as to whether computers have been properly disposed, and lack of encryption exposes the agency to a high probability that sensitive and personally identifiable information will be lost, stolen, or misused.

Recommendations

We recommend the Director, Office of Acquisition and Property Management and Chief Information Officer take the following actions:

1. Establish a uniform Department-wide system-controlled chain of custody property system for computers.

2. Incorporate information sanitization procedures in conjunction with property disposal procedures.

3. Require that the loss or theft of all computers be reported to the Department's Computer Incident Response Center.

4. Take immediate steps to encrypt all portable computers throughout the Department.

Appendix 1: Objective, Scope, Methodology, and Other Related Coverage

Objective, Scope, and Methodology

The objective of our evaluation was to determine whether the Department and bureau offices have effective controls over all desktop and laptop computers and Blackberries (and similar mobile devices) to reasonably ensure that these devices are adequately inventoried, safeguarded from damage, theft, or misuse, and properly disposed of at the end of their useful life. Our discussion throughout this report is limited to desktop and laptop computers as we found that Blackberries had IT security controls and limited storage capability.

We conducted our review from June 2008 to January 2009, which included the use of property or IT records provided by the Department and bureau offices to conduct limited testing of desktop and laptop computers. The scope of our review covered fiscal years 2007 and 2008. We conducted our evaluation in accordance with the *Quality Standards for Inspections* as put forth by the President's Council on Integrity and Efficiency. Accordingly, we included such tests of records and other procedures that were considered necessary under the circumstances. To accomplish our objective, we conducted the following activities:

- Reviewed applicable laws, regulations, OMB guidance, and Department and bureau policies.

- Reviewed Department property (i.e., NBC, which provides property management services to Departmental offices), bureau property, and IT records.

- Interviewed Department (i.e., NBC) and bureau office property and IT managers and specialists.

- Reviewed the Department's Annual Report on Performance and Accountability for fiscal years 2006 and 2007, including information required by the Federal Managers' Financial Integrity Act of 1982. We determined that none of the weaknesses reported by the Department directly related to our objective.

- Reviewed the Department's Strategic Plan and other related documents. We determined that the Department's IT plan, dated September 2007, stated that the Department's first priority was to ensure (1) private and sensitive information was adequately protected and (2) consistently secure identification, authentication, authorization and access of internal and external users to IT systems and network resources.

- Reviewed recent Congressional Hearings and found that in June 2007, the U.S. House of Representatives Subcommittee for Information Policy, Census, and National Archives met jointly with the Subcommittee on Government Management, Organization, Procurement, as well as the Committee for Oversight and Government Reform on the challenges facing computer security management, policy, and privacy. This hearing specifically addressed the implementation of the Federal Information Security

Management Act of 2002 and its effectiveness in improving computer security efforts. The overall sentiment was that despite some progress, the government's information systems remain vulnerable to security breaches and current policies and regulations need to be re-evaluated.

Other Related Coverage

The Office of Inspector General (OIG)issued a report, *Information Technology Systems Inventory*, dated August 2006, that concluded the need for improvements in the Department's controls over its information technology systems inventory. The GAO and other OIGs have conducted many audits on computer security. A few examples are as follows:

- June 2008, *Federal Agency Efforts to Encrypt Sensitive Information, but Work Remains* (GAO 08-525). GAO found that major agencies reported they had not yet installed encryption software on about 70 percent of laptops, computers, and handheld devices. All agencies had begun efforts to deploy encryption security, but none had any documented comprehensive guides for implementation activities.

- June 2008, *Indian Health Service Management Led to Millions of Dollars in Lost or Stolen Property* (GAO 08-727). GAO determined that Indian Health Service (IHS) was vulnerable to loss and theft of IT equipment and sensitive personal information due to its weak control environment and inadequate accountability over its inventory. Additionally, IHS did not (1) conduct annual inventories; (2) use receiving agents and designate property custodial officers; (3) maintain complete personal custody property records; and (4) use the accountable property management system.

- March 2007, *Internal Controls Over Computer Property at the Department's Counterintelligence Directorate* (DOE/IG-762). The Department of Energy's Office of Inspector General found that the Directorate was unable to provide assurance that computers for which it was accountable were appropriately controlled or adequately safeguarded against theft and loss. The Directorate was unable to locate 20 desktop computers that were listed on its property inventory and had difficulty locating a significant sum of computers because the inventory records were inaccurate.

Appendix 2: Sites Visited or Contacted

Sites Visited	
Agency	**Location**
National Business Center	Washington, D.C.
Office of Chief Information Officer	Washington, D.C.
Bureau of Indian Affairs	Herndon, VA Sacramento, CA Phoenix, AZ*
Bureau of Land Management	Washington, D.C. Sacramento, CA Folsom, CA
Bureau of Reclamation	Sacramento, CA Folsom, CA Denver, CO*
Fish and Wildlife Service	Arlington, VA Sacramento, CA
Mineral Management Service	Herndon, VA Camarillo, CA*
National Park Service	Washington, D.C. El Portal, CA
Office of Surface Mining	Washington, D.C.
U.S. Geological Survey	Sacramento, CA Menlo Park, CA Reston, VA*

**Denotes sites that were contacted but not physically visited.*

Report Fraud, Waste, Abuse And Mismanagement

Fraud, waste, and abuse in government concerns everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular area programs and operations. You can report allegations to us in several ways.

By Mail:	U.S. Department of the Interior Office of Inspector General Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240	
By Phone:	24-Hour Toll Free Washington Metro Area	800-424-5081 703-487-5435
By Fax:	703-487-5402	
By Internet:	www.doioig.gov	

Revised 06/08