PROTECTING THE PUBLIC: Treasury Departmental Offices' Control Over Computers Needs To Be Improved

OIG-03-038 **December 20, 2002**

Office of Inspector General

****

The Department of the Treasury

Contents

Audit Report 2

Results in Brief 2

Background 3

Finding and Recommendations 4

Controls Over Computers Should Be Strengthened 4
Recommendations 7

Appendices

Appendix 1: Objectives, Scope, and Methodology 9
Appendix 2: Management Response 10
Appendix 3: Major Contributors To This Report 12
Appendix 4: Report Distribution 13

Abbreviations

CIO	Chief Information Officer
DO	Treasury Departmental Offices
FY	Fiscal Year
GAO	General Accounting Office
OIG	Office of Inspector General
TOS	Treasury Office of Security and Critical Infrastructure Protection
OIG-OI	Office of Inspector General, Office of Investigations

December 20, 2002

Teresa Mullett Ressel
Acting Assistant Secretary for Management
and Chief Financial Officer

We conducted an audit of the Treasury Departmental Offices' (DO) controls over selected property items that, if lost or stolen, might compromise national security, the public's safety, or ongoing investigations. Sensitive property at DO included computers only.

We conducted this audit at the request of Senator Charles E. Grassley. Our specific objectives were to answer the following questions:

1. Are Treasury's inventory regulations sufficient to prevent loss or theft of its inventory?
2. Which Treasury bureaus are most susceptible to inventory loss or theft and why?
3. Have any Treasury inventory items been identified as lost or stolen within the last 3 fiscal years?
4. Does Treasury have a sufficient plan to recoup inventory that cannot be located?

The audit fieldwork was performed from June to September 2002. We interviewed DO officials and evaluated records and procedures. The scope of the review covered FY 1999 to FY 2001. See Appendix 1 for a more detailed description of the audit objectives, scope, and methodology.

Results in Brief

DO reported 11 computers lost or stolen during fiscal years (FY) 1999 through 2001, having a total value of at least $24,000. DO had written guidance, directives, and procedures for managing and safeguarding computers and the information they contained.

This minimized the risk of loss or theft. However, we noted DO did not conduct a periodic physical inventory of all its computers and we were unable to verify the number of computers reported lost or stolen during the audited period. These weaknesses increased the risk that computers could be lost or stolen without being timely detected.

We are recommending that the Assistant Secretary for Management and Chief Financial Officer ensure a complete physical inventory of all computers is conducted on a periodic basis. Also, the method for reporting lost or stolen computers should be re-evaluated to ensure all losses are reported to the proper authorities. This should include periodic reconciliations between the information maintained by the three reporting authorities: the Chief Information Officer (CIO), the Treasury Office of Security and Critical Infrastructure Protection (TOS), and the Office of Inspector General – Office of Investigations (OIG-OI).

DO concurred with the finding and recommendations. As a result, DO will perform a new physical inventory. DO will also work with TOS and the OIG-OI to draft procedures for periodic reconciliations of lost or stolen computers.

Background

Treasury is organized into two major components – Offices and Bureaus. The Treasury offices are composed of divisions headed by Assistant Secretaries, some of which report to Under Secretaries, and are primarily responsible for policy formulation and overall management of the Treasury Department. The Treasury bureaus make up 98 percent of the Treasury work force and are responsible for carrying out specific operations assigned to the Department.
Getronics Government Solutions is a contractor that provides information and communications technology solutions to DO. It is a provider of desktop outsourcing, network solutions, and information assurance services. The contractor's duties include conducting physical inventories of leased computers.

Three Treasury entities deal with lost or stolen computers: DO's CIO, TOS, and OIG - OI. The CIO is required to physically

inventory all computers and document those lost or stolen. DO personnel report lost or stolen computers directly to the TOS. TOS provides its reports to OIG - OI for potential investigation.

Finding And Recommendations

Controls Over Computers Should Be Strengthened

For FY 2001, DO reported it had 2,732 computers (1,845 desktops, 767 laptops, 120 handhelds). It also reported that 11 laptop computers were lost or stolen during our audit period. The total value for nine of these computers was $24,000. Cost information was not available for the other two losses. With the exception of two laptop computers, the remaining nine computers were identified as being in the possession of the contractor when stolen. Two other entities reported different totals for DO's lost or stolen computers. TOS reported 18 computer losses (14 laptops, 1 handheld, 3 docking stations), while the OIG - OI reported 21 losses (20 laptops, 1 handheld). Employees were not found financially liable for the missing computers. The Government assumed no liability for loss, theft, damage, or destruction (except for those resulting from its negligence, willful acts or omissions) of any asset (tangible or intangible) provided by the contractor in performance of the contract.

DO had: (1) written policies and procedures, which addressed the proper control and management of computer data; and (2) a contractor responsible for infrastructure management, maintenance, and asset management. These controls reduced the risk of loss or theft. However, DO had (1) a large number of computers dispersed worldwide, (2) no evidence of periodic physical inventories of all computers, and (3) incomplete inventory property records. These factors increased the risk of loss or theft. DO had controls that limited access to computer files and the DO computer network. These controls decreased the risk that sensitive data would be compromised, even if a computer were lost or stolen.

Written policies

DO had written policies that provided guidance on the control and management of computers. These policies included provisions for: reporting lost or stolen items, obtaining computers from departing employees, and disposing of excess property.

Quantity and geographic dispersion

DO personnel were assigned to locations worldwide, and used computers in the performance of their duties. A large number of computers dispersed over numerous geographic locations increased the risk that some of those items would be lost or stolen. Since DO's mission made it impractical to reduce the number of computers or centralize their location, it was important that a strong control environment be in place.

Physical inventories

DO had both leased and owned computers in its inventory. Currently, around 95 percent of DO's computers are leased with a target of December 31, 2002, for 100 percent leased. The contractor supported both leased and DO owned computers, which included performing perpetual inventories of all computers. During daily operations computers were installed, moved, added, or changed. At this time, contractor technicians ran the data management system's data collection software, which was used to update inventory records. However, if a computer was not installed, moved, added, or changed, it was assumed to be in the same location as identified in inventory records. The contractor also performed additional spot inventories in June and August 2002.

The contractor has recently implemented Navigator IT, a program which identifies assets connected to the DO Local Area Network. It collects hardware configurations (CPU, RAM, Hard Disks, Network and device information) and software installation data over the network and enables IT personnel to track and manage assets throughout their lifecycle. As a result of this newly established control, inventory accuracy will be increased, and the risk of loss or theft for computers will be reduced. However,

without performing a periodic physical inventory, there is no way to determine that DO has all its computers.

Inventory Records

Our review of the contractor's inventory records indicated there was a 10 percent error rate in their inventory list of DO computers. The types of errors we noted included missing serial numbers, and incorrect make and model information. A lack of descriptive data would prevent an adequate physical inventory, identification of losses, and delay or impede the subsequent investigation and/or potential recovery of the lost computers.

The accuracy of the inventory database was dependent on the scanning of every computer system during every installation, movement, addition, or change. Entries to the data management system were based on input provided by contractor personnel and others performing the actions on the equipment. Contractor policy stated that it was the responsibility of the person who was installing any asset to ensure that accurate inventory data was collected. As noted above, the contractor has recently implemented Navigator IT. When implemented, this will help increase inventory record accuracy. DO has subsequently provided evidence that the types of errors we noted in our review of the inventory records had been corrected. Accurate inventory records help to decrease the risk of loss or theft.

Data security

DO maintained information that is (1) classified[1] and (2) sensitive but unclassified.[2] DO used passwords to access its computers. All employees with access to classified and sensitive information and those officials authorized to classify documents were to receive mandatory formal security briefings annually. DO policy did not allow the connection of a laptop that processed classified information to an unclassified system, such as a Local Area

[1] DO defined classified information as information that is vital to the national security of the United States. It is clearly (but not always) marked Confidential, Secret, or Top Secret.

[2] DO defined sensitive information as information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Network or the Internet. It also did not allow the use of personally owned computers or software to process, access, or store classified national security, foreign intelligence, or Limited Official Use information either in a bureau facility, or private residence. DO policy stated that sensitive but unclassified and classified information may only be processed on government-owned laptops.

These controls over data security decreased the risk that sensitive information would be compromised, even if a computer was lost or stolen.

Reporting, investigating, and recouping lost or stolen computers

DO employees were required to immediately report lost or stolen computers assigned to them. During the audited period, the CIO reported 11 laptop computers lost or stolen. Two of these computers were assigned to specific individuals; those remaining were identified as stock (surplus) not assigned to specific personnel. The total value for nine of these computers was $24,000. Similar information was not available for the other two losses. While the CIO reported 11 losses, TOS and the OIG - OI reported DO with 18 and 21 lost or stolen computers, respectively. None of the computers were recovered, and TOS reported that for those computers it identified, no classified or sensitive information was lost. Because there was no reconciliation of information between the three interested entities, the numbers for losses and thefts varied. Consequently, we do not believe the number of computers DO reported lost or stolen is reliable.

Recommendations

The Assistant Secretary for Management and Chief Financial Officer should ensure that:

1. A complete physical inventory of all computers is conducted on a periodic basis.

2. The method for reporting lost or stolen computers is re-evaluated to ensure all losses are reported to the proper authorities. This should include periodic reconciliations between the CIO, TOS, and OIG – OI.

Management Comments

Management concurred with the finding and recommendations. When its new Asset Management database structure is deployed, a physical inventory will be performed. DO will also work with TOS and the OIG to draft procedures for periodic reconciliations of lost or stolen computers.

OIG Comments

We consider these recommendations to have management decisions with a target completion date of February 2003.

****

We appreciate the cooperation we received from DO officials during this audit. If you wish to discuss this report, you may contact me at (202) 927-5400 or Roberta N. Rickey, Regional Inspector General for Audit, at (312) 886-6300.

Marla A. Freedman
Assistant Inspector General for Audit

The overall objective of this audit was to address concerns Senator Charles E. Grassley raised regarding Treasury-wide inventory practices for items that if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. Our specific objectives were to answer the following questions:

(1) Are the bureau's policies and practices sufficient to prevent loss and theft?
(2) What items have been lost or stolen during FY 99 – 01?
(3) Does the bureau have a sufficient plan to recoup lost items?
(4) What improvements can be made to prevent future losses?

At DO, we considered computers to be a sensitive property item. Our audit scope covered FY 1999, 2000, and 2001 (from October 1, 1998, through September 30, 2001). To accomplish our objectives, we requested data on inventory levels at or near the end of FY 2001[3] and computers reported lost/stolen during FY 1999 – FY 2001; reviewed pertinent laws and regulations; reviewed written bureau policies; reviewed the latest physical inventory reports; reviewed documents related to lost/stolen computers; and interviewed officials.

We conducted our audit between June and September 2002 in accordance with generally accepted government auditing standards.

[3] The date of the reported inventory levels for the computers was October 1, 2001.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

NOV 22 2002

MEMORANDUM FOR MARLA A. FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Mike Parker, Acting Deputy Assistant Secretary (Information Systems) and Chief Information Officer

SUBJECT: Response to Draft OIG Report "Protecting the Public: Treasury DO Control over Computers needs to be improved"

The Office of Management and the Office of the Chief Information Officer (CIO) appreciate the opportunity to respond to the OIG report on Asset Management within the Departmental Offices (DO). The report indicates one finding and two recommendations. The Office of the CIO would like to clarify some points of information contained within the report.

The finding indicates that DO has not performed periodic physical inventories. As part of the transition to SEAT Management, the DO SEAT contractor, Getronics, performed an initial physical inventory in September 1999 and a further reconciliation inventory in February 2000. The OIG draft report does correctly indicate that additional spot inventories were performed in June and August of 2002 but neglects to mention the initial inventories. In addition, the SEAT contractor inherited a database from the outsourced government office that previously performed these functions. A number of errors were carried over from this original database (such as missing serial numbers or incorrect make/model) and were not corrected during the physical inventory. Since that time, the vast majority of these errors have been corrected.

As noted in the draft OIG report, the SEAT contractor will be converting to a new Asset Management tool. When this new database structure is deployed and integrated into the Getronics tool set at DO, a new physical inventory will be performed. Subsequent updates will then be performed via automated data collection across the DO network. Currently, this physical inventory is projected to be accomplished in February 2003. Additional physical inventories will be conducted based on industry best practices (as noted by the Gartner Group during its total cost of ownership review of the DO Seat Management implementation completed in September 2002) and by sampling the data error rate of the current installation collected via the network.

The report notes that Treasury DO is responsible for an inventory of computers worldwide. In fact, computers used by DO staff in overseas embassies are provided by the State Department, with DO technical staff providing software so that these overseas staff can link remotely and securely into the DO network by means of a Virtual Private

Network (VPN). In addition, there are several offices within the Washington DC Metro area that report to DO, yet receive no technical support from the CIO's office. Therefore, these computer systems are not captured within the database. These offices include the Community Development Financial Institutions (CDFI) fund, the Office of Asset Forfeiture, and the Office of Human Resources Enterprise Solutions (OHRES). Discussions are underway with OHRES to incorporate support into the current SEAT contract, at which time their inventory will be incorporated into the existing database. This fact is significant because it may account for the discrepancies in the numbers of lost and missing items reported by the various entities interviewed for the report.

The Office of the CIO concurs with the recommendation that periodic physical inventories should be performed and will implement this recommendation using the best practice sources noted above for the upcoming physical inventory. The office of the CIO also concurs with the recommendation that periodic reconciliations with the Treasury Office of Security and the Treasury Inspector General – Office of Investigations should occur and will draft procedures in concert with these entities to ensure compliance with the recommendation.

Technical questions about this response should be directed to Rory Schultz at 202-622-2829.

Central Region

Roberta N. Rickey, Regional Inspector General for Audit
Charles Allberry, Audit Manager
Bradley Mosher, Audit Manager
Claire Schmidt, Auditor

Department of the Treasury

Office of the Under Secretary of the Treasury for Enforcement
Office of the Assistant Secretary of the Treasury for Management and Chief Financial Officer
Office of Strategic Planning and Evaluations Management Control Branch
Office of Accounting & Internal Control
Office of Organizational Improvement

Treasury Departmental Offices

Assistant Secretary for Management and Chief Financial Officer
Assistant Program Manager, Operations and Services

Office of Management and Budget

OMB Budget Examiner