

U.S. Department of Labor

Office of Inspector General—Office of Audit

OFFICE OF THE CHIEF
INFORMATION OFFICER



INEFFECTIVE ACCOUNTING FOR SENSITIVE INFORMATION TECHNOLOGY HARDWARE AND SOFTWARE ASSETS PLACES DOL AT SIGNIFICANT RISK

Date Issued:
Report Number:

March 31, 2011
23-11-001-07-001

**U.S. DEPARTMENT OF LABOR
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT**

BRIEFLY...

Highlights of Report Number: 23-11-001-07-001
Ineffective Accounting for Sensitive Information
Technology Hardware and Software Assets Places
DOL at Significant Risk.

WHY READ THE REPORT

The U.S. Department of Labor (DOL), Office of Inspector General (OIG), conducted an audit of the inventory of DOL's sensitive IT hardware and software. The audit objective was to determine if the Department accounts for its inventory of sensitive IT assets

The audit covered DOL's primary inventory processes, including Procurement, Asset Distribution and Assigned Accountability, Disposal, Reconciliation, and Inventory Update from October 1, 2006 thru July 6, 2010.

WHY OIG CONDUCTED THE AUDIT

The Office of Inspector General (OIG) is issuing this report due to concerns over recent, high-profile instances of laptop thefts and data breaches, the Federal government has been concerned about Federal agencies' ability to account for their sensitive Information Technology (IT) assets. To push agencies to examine their risks and make substantial security improvements to address these concerns, in 2010 the Office of Management and Budget (OMB) developed an outcome-focused metric for information security performance for Federal agencies designed in part to ensure they are accountable for sensitive IT assets.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full agency response, go to:
<http://www.oig.dol.gov/public/reports/oa/2011/23-11-001-07-001.pdf>

MARCH 2011

INEFFECTIVE ACCOUNTING FOR SENSITIVE INFORMATION TECHNOLOGY HARDWARE AND SOFTWARE ASSETS PLACES DOL AT SIGNIFICANT RISK.

WHAT OIG FOUND

The OIG found DOL cannot account for its sensitive IT assets. From our sample, we could not physically locate approximately 50 percent of assets recorded in the E-Property Management System (EPMS), and could not find, and were not provided any records for, approximately 14 percent of IT assets we located on the floor. Furthermore, The Department could not locate approximately 71 percent of IT assets that had been procured using the E-Procurement System (EPS). In addition, Department security officials could not determine whether sensitive data (e.g., personally identifiable information (PII)) existed on 377 sensitive IT assets in the Office of the Assistant Secretary for Administration and Management (OASAM) that had been reported lost, missing, or stolen. The Department could not determine if these items — which included laptops, desktops, printers, blackberries, and a server — represented a potential information security breach.

DOL confirmed it had not certified its IT inventory since 2007. On January 5, 2010, the Assistant Secretary for Administration and Management required all 24 program agencies to certify its IT inventories. As of July 8, 2010, 11 program agencies had not certified their inventories in the EPMS, the official system of record, and 2 agencies had certified their inventories outside of the EPMS. The remaining 11 program agencies had certified their IT inventory as complete and accurate. However, as noted throughout this report, substantial errors in the inventory data tested were found.

Also, written department-wide policy or procedures that should govern how program agencies are to dispose of IT assets did not exist.

Finally, we noted that one agency developed its own inventory system — duplicating EPMS — without receiving authorization from the Department to waive the required use of EPMS.

WHAT OIG RECOMMENDED

The OIG made six recommendations covering enforcing accountability over current policies and developing policies for areas such as disposal that presently lack coherent policy; establishing a viable inventory management system; assessing impact of reported lost, missing, or stolen assets; consolidating any duplicative inventory systems to realize cost savings; and strengthening inventory and security controls. Management agreed with the spirit of the recommendations and plans to take corrective actions.

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Assistant Inspector General’s Report	1
Objective — Can the Department account for its inventory of sensitive IT assets?	3
<i>DOL’s inventory system failed to properly account for IT sensitive assets in all five phases of the inventory process.</i>	3
Finding — DOL’s inventory controls and processes are ineffective	3
Recommendations	14
Exhibits	
Exhibit 1 Unassigned Items by Agency as of July 2010 (from EPMS Sample Universe).....	18
Exhibit 2 OASAM Inventory Analysis of Lost/Stolen/Missing IT Assets	20
Exhibit 3 Agencies’ Ability to Reconcile EPS IT Asset Information to EPMS	22
Exhibit 4 Reconciling Sensitive IT Assets from Floor to EPMS Inventory	24
Exhibit 5 Reconciling Sensitive IT Assets from EPMS to Floor.....	26
Exhibit 6 Missing EPMS IT Asset Data.....	28
Appendices	
Appendix A Background	32
Appendix B Objective, Scope, Methodology, and Criteria	34
Appendix C Acronyms and Abbreviations	40
Appendix D OCIO Response to Draft Report	42
Appendix E Acknowledgements	46

PAGE INTENTIONALLY LEFT BLANK

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210



March 31, 2011

Assistant Inspector General's Report

Mr. T. Michael Kerr
Chief Information Officer
U.S. Department of Labor
200 Constitution Avenue, N.W
Washington, D.C. 20210

Due to concerns over recent, high-profile instances of laptop thefts and data breaches, the Federal government has been concerned about Federal agencies' ability to account for their sensitive Information Technology (IT) assets. To push agencies to examine their risks and make substantial security improvements to address these concerns, in 2010 the Office of Management and Budget (OMB) developed an outcome-focused metric for information security performance for Federal agencies designed in part to ensure they are accountable for sensitive IT assets.

In order to gauge the U.S. Department of Labor's (DOL) ability to account for its inventory of sensitive IT assets, the Office of Inspector General (OIG) conducted a performance audit of the inventory of DOL's sensitive IT hardware and software. Our audit objective was to answer the following question:

Can the Department account for its inventory of sensitive IT assets?

The audit covered DOL's primary inventory processes, including procurement, asset distribution and assigned accountability, disposal, reconciliation, and the update of inventory in the Department's official system of record, the E-Property Management System (EPMS). Our scope was the period October 1, 2006, through July 6, 2010, and was limited to selected sensitive IT assets that have a higher security-risk potential due to loss or theft of the asset and the resulting potential harm that may occur.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions that are consistent with our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our objective, scope, methodology, and criteria are detailed in Appendix B.

RESULTS IN BRIEF

DOL cannot account for its sensitive IT assets. From our sample, we could not physically locate approximately 50 percent of assets recorded in the EPMS, and could not find, and were not provided any records for, approximately 14 percent of IT assets we located on the floor. Furthermore, The Department could not locate approximately 71 percent of IT assets that had been procured using the E-Procurement System (EPS). In addition, Department security officials could not determine whether sensitive data (e.g., personally identifiable information (PII)) existed on 377 sensitive IT assets in the Office of the Assistant Secretary for Administration and Management (OASAM) that had been reported lost, missing, or stolen. The Department could not determine if these items — which included laptops, desktops, printers, blackberries, and a server — represented a potential information security breach. Our concern over these reported lost, missing, or stolen items is elevated since OASAM is responsible for human resources and budget operations, and manages a large IT center.

DOL confirmed it had not certified its IT inventory since 2007. On January 5, 2010, the Assistant Secretary for Administration and Management required all 24 program agencies to certify its IT inventories. As of July 8, 2010, 11 program agencies had not certified their inventories in the EPMS, the official system of record, and 2 agencies had certified their inventories outside of the EPMS. The remaining 11 program agencies had certified their IT inventory as complete and accurate. However, as noted throughout this report, we found substantial errors in the inventory data tested.

Also, written department-wide policy or procedures that should govern how program agencies are to dispose of IT assets did not exist.

Finally, we noted that one agency developed its own inventory system — duplicating EPMS — without receiving authorization from the Department to waive the required use of EPMS.

The obvious and systemic control deficiencies we identified are the result of DOL's inventory system's lack of proper accountability of IT sensitive assets in all five phases of the inventory process — procurement, inventory distribution and accountability, disposal, reconciliation, and inventory update — and the Chief Information Officer's (CIO) lack of oversight. Without significant improvements in oversight, accountability, and inventory controls, the Department risks the potential of eroding the public's trust should an undetected information security breach occur.

We recommended the CIO enforce accountability over current policies and develop policies for areas such as disposal that presently lack coherent policy. In addition, the CIO must ensure that information is updated in a viable inventory management system, assess impact of reported lost, missing, or stolen assets, consolidate any duplicative inventory systems to realize cost savings, and strengthen inventory and security controls.

In responding to our draft report, the Deputy Assistant Secretary for Administration Management stated that nothing in their response is intended to suggest that management does not take seriously the recommendations of the OIG and will take corrective actions. Management acknowledged that there are deficiencies in the property management system; however, management indicated that the OIG report contained erroneous assumptions in the following areas: 1) use of the term “Sensitive” IT Assets, 2) absence of EPS and EPMS functionality descriptions, 3) lack of relevance of EPS errors to EPMS, and 4) the mischaracterization of a Significant Deficiency. OIG has responded to each of these issues in the body of the report. In addition, management responded that recommendation number six, “Integrate a reliable electronic procurement system with a viable inventory system along with the financial systems to ensure seamless interoperability,” goes beyond the scope of the audit and the [OIG] recommendation should be to implement processes to account for its assets. OIG retains its recommendation since the inventory processes audited have numerous deficiencies. Automation, along with integration, would be the best approach to ensuring DOL can account for its inventory.

The agency’s entire response is contained Appendix D.

RESULTS AND FINDINGS

Objective — Can the Department account for its inventory of sensitive IT assets?

DOL's inventory system failed to properly account for IT sensitive assets in all five phases of the inventory process.

Finding — DOL’s inventory controls and processes are ineffective

The control deficiencies identified in the inventory processes of 1) procurement, 2) inventory distribution and accountability, 3) disposal, 4) reconciliation, and 5) inventory update, demonstrate the degree to which DOL’s inventory process is ineffective, and to which management has been inadequate over the years.

1) Procurement

Based upon analysis of the EPS, we found no evidence of controls that ensure proper recording of all IT assets. From our sample of 432 procurement line items that we provided to selected agencies, which included sensitive IT assets, these agencies could not locate 308 line items (approximately 71 percent) of IT assets that were procured using the EPS.

When requested, the Department could not provide a complete listing of sensitive IT assets with their associated dollar amounts procured through the EPS. As such, we performed a word query of the asset/service description field for IT-related assets within EPS. EPS Category Code 4, which is utilized to track Electronic and Information Technology (EIT) procurements, only listed a total of 1,484 IT procurements costing nearly \$1 million¹. However, we identified 9,380 procurements associated with IT items costing nearly \$280 million² that were listed under Category Code 1 (Unclassified procurements), which did not have the IT assets classified as EIT procurements; nor were they properly classified as EIT – Category Code 4.

The EPS contains an asset/service description field that allows users to characterize the assets/services being procured and select the EIT classification code. However, when users do not select the proper EPS asset /service classification code — in this case, IT procurements as Category Code 4 — the EPS (as a default) records the asset/service being procured as unclassified – Category Code 1.

The EPS IT asset data showed various data input errors related to procurement. Our review of the four largest procurements determined that the Department had not corrected a coding error, in which a procurement of approximately \$1 million was actually coded as \$77 million.

Management believes the above error lacks relevance to the Department's inventory system, since EPS is not part of the Department's inventory system. OIG used EPS information as a result of the Department's inventory system starting with the procurement of goods and services. The EPS is the primary system used for that purpose; albeit there are also purchases using purchase cards. Use of the EPS data is relevant, since 9,380 procurements associated with IT items were initiated and completed using EPS. Inventory reconciliations, when performed, should use accurate EPS information to determine what sensitive IT equipment was procured and continues to be in use and managed.

In addition, we identified 204 instances from our population of 9,380 procurements associated with IT items that had negative order quantity amounts, and 1,105 instances of where IT items had a unit price of zero dollars. These errors further corrupted the accuracy of the procurement data within EPS and subsequently the inventory of sensitive IT assets within the EPMS.

Differentiating sensitive IT hardware and software from other IT procurements is not possible using the current EPS coding structure. EPS does not differentiate whether an item being procured is a sensitive IT asset such as a laptop, printer, or software license, or an office supply item such as an ink cartridge. As a result, managing the procurement of sensitive IT hardware and software would be extremely difficult using the EPS without a high degree of human intervention and manipulation of text data.

¹ Actual dollar amount was \$997,940

² Actual dollar amount was \$279,460,380

Since the Department could not provide a list of sensitive IT assets, we identified procurements of these assets using the process described in the Methodology section of this report (see Appendix B). This defined universe included 2,406 procurements of sensitive IT assets costing more than \$46.7 million³. These procurements were further categorized as follows: 1,423 unclassified procurements costing nearly \$46 million⁴; and 983 EIT procurements costing \$812,064. From these procurements, we selected the following two statistical samples totaling 432 procurements to determine if they were recorded in EPMS:

- 270 IT procurements from the 1,423 unclassified procurements. From this sample, we identified 217 procurements that were not recorded in EPMS. We projected there were about 1,123 unclassified procurements that were not recorded in EPMS totaling about \$21 million⁵.
- 162 IT procurements from the 983 EIT procurements. From this sample, we identified 91 procurements with errors. We projected there were about 551 EIT procurements of sensitive IT assets that were not recorded in EPMS totaling about \$277,000⁶.

In accordance with Department of Labor Manual Series (DLMS) 9, Chapter 303, *Management & Accountability of Information Resources*, all DOL agencies are to maintain an accurate inventory of their information resources in compliance with the law.

2) Inventory Distribution and Accountability

We found that, of the IT assets we tested, approximately 24 percent were not assigned to owners, and the owners' names were not recorded in the EPMS by the responsible program agency's Accountable Property Officers (APO). Without this information in EPMS, the Department and its program agencies cannot utilize EPMS to properly manage the inventory and hold owners accountable for their IT assets.

We defined a universe of 29,106 EPMS records from the July 6, 2010, EPMS database to verify IT asset records. We identified 6,867 IT assets (23.6 percent), costing more than \$1.2 million⁷ that had unassigned owners (see Exhibit 1). While most program agencies we reviewed did not consistently record owners of IT assets in the EPMS, the following program agencies had the greatest percentage of unassigned owners:

³ Actual dollar amount was \$46,769,630

⁴ Actual dollar amount was \$45,957,566

⁵ This projection was achieved with a confidence level of 95 percent and a sampling precision of plus or minus 4.67 percent.

⁶ This projection was achieved with a confidence level of 95 percent and a sampling precision of plus or minus 6.92 percent.

⁷ Actual dollar amount was \$1,221,747

Unassigned Owners of Sensitive IT Assets in EPMS			
Agency	Number of Sensitive IT Assets Tested	Number of Sensitive IT Assets without an Assigned Owner	Percent of Sensitive IT Assets without an Assigned Owner
OPA	126	56	44
ETA	2,334	804	34
OSHA	3,795	1,228	32
ESA	14,123	3,842	27

The Department's DLMS 2, Chapter 100, *Property Management*, requires agencies to accurately record in the EPMS the existence, location, and assignment of all assets. In addition, the APOs are responsible for certifying annual inventories are accurate and complete within the EPMS.

3) Disposal

Agencies did not consistently update EPMS to record the disposal of sensitive IT assets. OASAM's Business Operation Center's (BOC), Office of Administrative Services (OAS), was responsible for the Department's disposal guidelines, however, there was no written, approved department-wide policy that existed to govern how program agencies should dispose of IT assets. BOC OAS offers all program agencies disposal services; however, program agencies did not consistently utilize BOC OAS or record the disposal of sensitive IT assets. Without a department-wide policy and related procedures, the potential exists that IT equipment will not be properly sanitized prior to its disposal, thereby increasing the risk of information security breaches that could go undetected.

To examine the disposal of sensitive IT assets in EPMS, we reconciled EPMS disposal information to BOC OAS disposal records. Based on a comparison of June 1, 2010, EPMS disposal data to disposal records provided by BOC OAS, we identified an overall discrepancy of 1,576 records pertaining to disposal of IT assets. The examples below highlight some of these discrepancies:

- The Mine Safety and Health Administration (MSHA) stated it adhered to its own agency-specific disposal procedures and did not rely on BOC OAS. MSHA reported in EPMS disposal of 15 IT assets (11 printers and 4 laptops) on October 1, 2007. However, as of October 19, 2007, BOC OAS disposal records indicated that MSHA did utilize BOC OAS in disposing of 6 IT assets (2 central processing units (CPU), 4 printers, and no laptops).
- The Occupational Safety and Health Administration (OSHA) stated that it used the BOC OAS disposal services. OSHA reported in EPMS disposal of 10 laptops on October 3, 2007. However, BOC OAS disposal records showed no activity until July 16, 2009, at which time OSHA indicated it disposed of 36 laptops.

- The Bureau of Labor Statistics (BLS) stated it used the BOC OAS disposal services. BLS did not report any disposal activity in EPMS from October 1, 2009, through June 1, 2010. However, BOC OAS disposal records indicated that BLS disposed of 309 CPUs on May 7, 2010.

These examples of discrepancies in agencies' EPMS disposal records and the Department's IT asset disposal records indicated the CIO had significant difficulty assuring agencies were properly sanitizing covered IT assets⁸ prior to disposal. Without this assurance, the Department's systems and sensitive information, including personally identifiable information, were at increased risk of being compromised.

For example, we identified that 30 OASAM cost centers reported 202 desktops, 51 laptops, 115 printers, 8 blackberries, and 1 server as lost, missing or stolen during OASAM's 2010 IT inventory recertification. (See Exhibit 2.) Neither OASAM nor the Office of the Chief Information Officer (OCIO) provided evidence showing that an analysis or investigation was performed to determine whether appropriate breach procedures needed to be initiated and/or adhered to. As a result, the Department had no way to determine if missing IT assets represented a potential information security breach. OASAM's inability to maintain complete records is of particular concern because it performs Department-wide human resources, budget, and IT-related functions. It is likely that IT assets used in performing these functions may contain PII and/or sensitive information.

In following up on our expressed concerns, an OAS official stated its office took a random sample of 15 reported OAS lost/missing/stolen sensitive IT assets and determined the assets were disposed of properly. Upon further inquiry, OAS provided no evidence and/or documentation to corroborate its efforts and final determination that departmental breach policies did not have to be implemented.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88 – Guidelines for Media Sanitization encourages agencies to develop and use local policies and procedures in conjunction with its guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information. NIST SP 800-53 states that offices shall track, document, and verify media sanitization and disposal actions.

DOL's PII Breach Notification Plan states that "reporting requirements do not distinguish between potential and confirmed breaches." They also state:

When incidents involve PII, agency Information Security Officers (ISO) must follow DOL Computer Security Handbook (CSH) Volume 8, *Incident Response Procedures*, for notifying DOL Computer Security Incident Response Capability (DOLCSIRC) using the standard incident reporting form. Agency ISOs are responsible for notifying DOLCSIRC of any

⁸ Covered IT assets include those with data storage capability, e.g., servers, laptops, desktops, PDA's, printers, and copiers.

suspected breaches of PII within their agency; DOLCSIRC will then document the incident in the DOL incident tracking system and notify the United States – Computer Emergency Readiness Team (US-CERT) within 1 hour of notification. DOLCSIRC will also notify the DOL PII Breach Notification Team.

Management believes that the use of the term “Sensitive” IT assets is misused in the report. Management defined in their response that security sensitivity of an asset is based on the type of data stored or processed on the asset, as well as the function of the asset. OIG’s audit work did not specifically evaluate the security sensitivity of an IT asset, rather the work assessed whether the Department had effectively accounted for its sensitive IT assets, as defined by departmental policy. OIG identified deficiencies in the inventory processes such as not physically locating approximately 50 percent of EPMS sampled sensitive IT assets, agencies not recording owners of the IT assets, agencies not performing inventory reconciliations, and agencies not submitting accurate inventory certifications. Overall, these deficiencies have the potential to exposing the agencies to unnecessary risk, since the IT assets OIG audited were sensitive IT assets that have the capabilities of storing and accessing sensitive systems and information.

4) Reconciliation

The Department did not have written policies and procedures for performing reconciliations using its EPS procurement and EPMS inventory and disposal information. Without inventory reconciliation policies and procedures, the Department and agencies could not accurately and completely account for their IT assets. To assess the effectiveness of the IT reconciliation process, we performed verification tests in several ways, as follows:

- Using EPS to request that program agencies confirm IT asset existence and provide the descriptive information required in the EPMS.
- Conducting walk-throughs of program agency offices to physically confirm that sampled assets from locations in related offices (floor) were recorded in the EPMS inventory.
- Verifying IT assets from the EPMS inventory to IT assets physically found on the floor to confirm that these sampled assets in the EPMS inventory were located where specified.

We defined an EPS universe of procurements to perform verification testing of IT asset procurements. This defined universe comprised 2,406 procurements, totaling more than \$46.7 million⁹.

⁹ Actual dollar amount was \$46,769,630

Testing Agencies’ Ability to Reconcile EPS Sensitive IT Assets – We selected a sample of 231 procurements and provided the agencies with their respective inventory information. We requested each agency to confirm the assets’ existence and the descriptive information required to be recorded in EPMS. The agencies were unable to provide all of the requested data, including EPMS-required asset information, i.e., asset ID number, barcode number, serial number, model number, manufacturer, status description, asset assignment, location, and inventory class (see Exhibit 3). The chart below highlights which agencies had the most difficulty in providing all of the required asset information:

Agencies That Had the Most Difficulty Reconciling EPS Sensitive IT Asset Information to EPMS				
Program Agency	Number of selected samples	Number of samples for which data request was satisfied	Number of samples for which data request was not satisfied	Percent of samples for which data request was not satisfied
OASAM	45	0	45	100
OFCCP	28	0	28	100
OWCP	22	0	22	100
WHD	22	0	22	100
EBSA	9	2	7	78
OSHA	48	19	29	60

Conducting Walk-Throughs and Testing IT Assets from Floor to EPMS Inventory – We performed on-site testing in the program agencies by conducting a walk-through of the program agencies’ offices and judgmentally selecting 270 sensitive IT assets from locations on the floor to reconcile back to the EPMS inventory. Although some agencies did not have issues with reconciliation, based on the test results, the Department did not have any records in the EPMS for 38 floor items (14 percent) (see Exhibit 4). Program agencies showing greater reconciliation problems are shown below:

Reconciling Sensitive IT Assets from Floor to EPMS Inventory			
Program Agency	Selected Items	Items Not Located in EPMS	Percent Missing
ETA	30	18	60
OFCCP	25	7	28
OWCP	25	4	16
DITMS	20	3	15

Testing Sensitive IT Assets from EPMS Inventory to Floor - We tested a sample of 251 IT assets from a defined universe of 29,106 EPMS IT assets. We verified whether they existed at the location specified in EPMS. Of this sample, 125 assets (50 percent) recorded in EPMS could not be located (see Exhibit 5). The program agencies that had the most difficulties in its inventory are highlighted in the following table:

Program Agencies with the Most Difficulties Reconciling Sensitive IT Assets from EPMS to Floor			
Program Agency	Total Number of Sensitive IT Assets	Number of Sensitive IT Assets Not Located	Percent of Sensitive IT Assets Not Located
OASAM	38	30	79
OFCCP	42	23	55
WHD	29	15	52
OWCP	44	21	48
MSHA	19	8	42
ETA	41	17	41

Since the Department has not completed the integration of these systems, reconciliation of IT inventory assets will likely continue to be inaccurate and incomplete.

5) Inventory Update

Prior to the start of our audit, the Department had not certified its inventory of IT assets since 2007. On January 5, 2010, the Assistant Secretary for Administration and Management required each program agency to certify its inventory and update EPMS to record and track the assets. As of July 8, 2010, 11 program agencies did not certify their inventories in EPMS and 2 agencies certified their inventories outside of EPMS. The remaining 11 program agencies certified their IT inventories as complete and accurate. However, as noted throughout this report, we found substantial errors in the inventory data tested.

Without full and accurate accounting of the Department's IT assets, the risks to DOL's information security program, systems, and information — in particular, sensitive information — is unnecessarily increased.

IT Software Inventory was Not Updated in EPMS – Overall, program agencies were not updating EPMS with commercial off-the-shelf software license asset information. We identified software items in EPMS for the Employment and Training Administration (ETA), Employment Standards Administration (ESA), OSHA, and OASAM. However, the actual number of listed assets in EPMS was very low. When confirming this information with program agency representatives, they confirmed that their respective inventories of software licenses in EPMS were incomplete. Additionally, software licenses were not found in EPMS for the Employee Benefits Security Administration (EBSA), BLS, and MSHA.

IT Hardware Inventory was Not Updated in EPMS – Program agencies were not updating EPMS with hardware information. Using the agencies' 2010 inventory certifications and the updated data in EPMS, we found that 21 percent of the required EPMS data fields were left blank (see Exhibit 6). These discrepancies highlight the Department's inability to determine an accurate inventory of IT hardware.

BLS Opted Out of EPMS – BLS did not adhere to departmental requirements to properly maintain inventory data within the EPMS because the agency had created and implemented a separate, unauthorized Asset Management System (AMS). All BLS inventory data in EPMS, which consisted of 894 IT assets costing more than \$3.8 million¹⁰, were “test” data. BLS provided a series of emails from OCIO, OASAM and BLS officials that acknowledged BLS developed AMS for the purpose of not using DOL’s EPMS while DOL was working toward an integrated solution for inventorying its assets. BLS informed the Department it would have a separate AMS, however, BLS did not receive an exemption from maintaining a proper inventory in the Department’s EPMS, and the Department did not enforce BLS’ compliance with current inventory policies.

Although the Department was aware that BLS was utilizing the AMS as an inventory system running parallel to EPMS, the Department was not aware that BLS updated the EPMS with test data. The inclusion of test data in a production system risks the corruption of the EPMS and places the Department at risk for misusing the test information for decision-making and assessing risks to its information security program. OASAM officials stated they planned to remove this test data from the EPMS, but did not provide documentation as to when this action will be completed. Nonetheless, the BLS AMS contradicted the purpose of having one central departmental inventory system. The elimination of BLS’s AMS would present the Department with a consolidation opportunity and cost savings by eliminating the duplication of an administrative system.

BLS officials maintained that the AMS was properly categorized under the Federal Information Processing Standards (FIPS) 199, and was certified and accredited under its Management of Information Systems infrastructure security package. BLS provided a system baseline diagram of its Management of Information Systems (MIS), which was comprised of a number of financial, human resources, and other administrative applications, which included the AMS. However no documentation was provided that categorized the system as a high, medium, or low risk system, as required by FIPS 199.

DLMS 2, Chapter 100 *Property Management*, requires all DOL agencies and offices nationwide to utilize EPMS to keep inventory of accountability property, with the exception of the Office of Job Corps (JC). In addition, the policy requires program agencies’ APOs to be responsible for certifying annual inventories that are accurate and complete within EPMS.

DLMS 9, Chapter 303, *Management & Accountability of Information Resources*, states that all DOL agencies will maintain an accurate inventory of their information resources in compliance with the law, including the E-Government Act (including the Federal Information Security Management Act (FISMA)), the Paperwork Reduction Act, the Clinger-Cohen Act, and related CIO and OMB guidance

¹⁰ Actual dollar amount was \$3,884,152

The DOL CSH, Volume 4, Section I, C&A Policies, Subsection 1.5, requires that all DOL information systems undergo the certification and accreditation process and be authorized to operate before being placed into the production environment. Minor applications may be included in the certification and accreditation of a major information system; otherwise, they must undergo a separate certification and accreditation process.

Reasons for the Systemic Conditions in the Inventory Process

We identified three primary reasons why management of DOL's inventory of Sensitive IT assets was ineffective:

- the inventory system was not integrated,
- not all program agencies used or relied on EPMS, and
- OCIO did not perform monitoring and oversight.

Each of these is explained further below.

- **The Inventory system was not integrated.**

There was no electronic interconnection between EPS and EPMS. A post-implementation review of the EPMS system commissioned by OASAM/BOC in December 2006 recommended that EPS be integrated with EPMS to provide a mechanism to streamline the management of property from its inception. This same review also recommended EPMS to have connectivity to the personnel database for automated updates of personnel status. OASAM EPMS Risk Assessment, as early as 2007, identified and emphasized the requirement that EPMS integrate fully with both EPS and financial systems to ensure seamless interoperability. Not implementing the recommendation and meeting the system requirement now makes it difficult, if not impossible, to account for all current assets, disposals, and the creation of a new, updated inventory, including sensitive IT assets. Program agencies had created unofficial records, followed ill-advised practices, and developed an unauthorized inventory system, which placed added stress on the Department's information security program.

Management believes the statements above are factually correct, but that there is no requirement that the systems be connected and electronic integration of the two systems is not part of the design. OIG was not implying the Department is required to have the systems connected and integrated to account for the Departments' IT assets. OIG was making the point that the Department had already received information that EPS be integrated with EPMS to provide a way to account for IT assets from its inception, but did not act on the information.

- **Not all program agencies used or relied on EPMS.**

Based upon response to an OIG survey that asked each program agency to disclose its inventory methods and practices, the results showed that not all

program agencies were using EPMS as their primary inventory method/property system to track and record inventory. Four of 19 program agencies who completed the survey stated they did not use the Department's EPMS system to track and record inventory, including IT assets. Following is a description of the four agencies' methods of recording and tracking their IT assets:

- Office of the Secretary (OSEC) and the Adjudicatory Boards (Administrative Review Board, Benefit Review Board, and Employees' Compensation Appeals Board) stated that they used an Excel spreadsheet.
- ETA stated it used a Computer Associates IT client system.
- BLS stated it used an agency-specific E-Property system, AMS.
- **OCIO did not perform Monitoring and oversight.**

The OCIO had not implemented required reviews of the program agencies' information resources accountability and inventory practices and procedures to ensure they met all legal requirements.

The Department's DLMS 9 - Chapter 300, *Management & Accountability of Information Resources*, Paragraph 306.A, requires the OCIO to be responsible for performing periodic review of the program agencies' information resources accountability and inventory practices and procedures to ensure each met all legal requirements.

DOL's information security program has worsened as a result of the deficiencies identified in this report, as well as several years of neglect in certifying their inventories to assure DOL's inventory of assets, especially IT assets, were fully accounted for through management of a viable asset inventory system. Without significant improvements in oversight, accountability, and inventory controls, the Department risks serious harm to its systems and information, including the potential of eroding the public's trust should an undetected information security breach occur. The issues identified in this report present management with serious challenges in lowering security risks and improving the management of sensitive IT assets and its data. The impact from these identified issues on DOL's information security program and related control vulnerabilities meet the definition of a significant deficiency under FISMA.

Management's view is that the information provided does not warrant the classification of a significant deficiency. OIG's determination, using OMB M-10-15 dated April 21, 2010, determined that inventory of sensitive IT assets was not a design flaw; however, the deficiency was identified across multiple systems, had the potential of compromising agency information systems and other resource operations or assets, and that a prudent official would conclude that the

deficiency is at least a significant deficiency. A significant deficiency is identified if only one of these factors is determined to exist.

RECOMMENDATIONS

Because of the significant deficiency identified in managing sensitive IT assets, we recommend the CIO immediately take the following actions:

1. Assess and take appropriate measures to ensure reports of lost, missing, or stolen sensitive IT assets have not resulted in loss of sensitive (PII) information in accordance with US-CERT and DOL Information Breach Policy and Procedures.
2. Perform a full inventory of the Department's IT assets that is accurate and complete including an update of the information into a viable inventory management system.
3. Consolidate all inventory systems throughout DOL to eliminate duplication, realize cost savings, and strengthen inventory and security controls over IT assets.
4. Perform required reviews of program agencies' inventory practices and procedures to ensure full participation in the inventory process across the Department and compliance with Federal information system requirements.
5. Develop policies for disposal of sensitive IT assets that presently lack coherent policy.
6. Integrate a reliable electronic procurement system with a viable inventory system along with the financial systems to ensure seamless interoperability.

We appreciate the cooperation and courtesies that departmental and program agency personnel extended to the Office of Inspector General during this audit. OIG personnel who made major contributions to this report are listed in Appendix E.



Elliot P. Lewis
Assistant Inspector General
for Audit

PAGE INTENTIONALLY LEFT BLANK

Exhibits

PAGE INTENTIONALLY LEFT BLANK

Exhibit 1

Unassigned Items by Agency as of July 2010 (from EPMS Sample Universe)

Agency	Number of Items Total	Number of Items Missing	Percentage Unassigned of Agency Total	Percentage Unassigned of Dept Total	Total Cost of Unassigned Items
Adjudicatory Boards	245	0	0	0	\$0.00
Assistant Secretary for Policy	12	0	0	0	\$0.00
Bureau of International Labor Affairs	142	20	14.1	0.1	\$0.00
Bureau of Labor Statistics	786	60	7.6	0.2	\$102,536.00
Employee Benefit Security Administration	477	47	9.9	0.2	\$466.31
Employment and Training Administration	2334	804	34.4	2.8	\$586,065.05
Employment Standards Administration	14123	3842	27.2	13.2	\$457,338.53
Mine Safety and Health Administration	1135	4	0.4	0	\$2,774.00
Occupational Safety and Health Administration	3795	1228	32.4	4.2	\$6,026.00
Office of Administrative Law Judges	332	1	0.3	0	\$239.00
Office of Congressional and Intergovernmental Affairs	43	4	9.3	0	\$0.00
Office of Disability Employment Policy	16	0	0	0	\$0.00
Office of Public Affairs	126	56	44.4	0.2	\$0.00
Office of Small Business Programs	10	0	0	0	\$0.00
Office of the Asst Secretary for Admin and Management	3332	374	11.2	1.3	\$49,217.96
Office of the Chief Financial Officer	309	14	4.5	0	\$12,699.00
Office of the Inspector General	341	144	42.2	0.5	\$0.00
Office of the Secretary	194	0	0	0	\$0.00
Office of the Solicitor	890	196	22.0	0.7	\$1,619.85
Office of Veterans' Employment and Training	204	43	21.1	0.1	\$0.00
Office of Security and Emergency Management	84	2	2.4	0	\$0.00
Women's Bureau	176	28	15.9	0.1	\$2,765.40
Total	29106	6867		23.60	\$1,221,747

PAGE INTENTIONALLY LEFT BLANK

Exhibit 2

OASAM Inventory Analysis of Lost/Missing/Stolen IT Assets

Cost Center Number	Cost Center Names	Desktop	Laptop	Printer	Blackberry	Server
6520	OAS -Office of Space Management	18	1	4	0	0
6510	OAS -Office of Customer Services	0	0	1	0	0
6085	Division of Engineering -FPB Real Property operations and Recurring Property Operations	8	0	2	0	0
6500	OAS -Office of the Director	13	2	6	0	0
6583	Division of Mail and Distribution Services (DMDS)	8	0	5	0	0
6084, 6581	6084 is Division of Building Management and 6581 is Office of Facilities Management	16	0	15	0	0
6200	BOC	6	12	1	0	0
6561	Office of Printing and Supply Management (OPSM)	25	1	5	2	0
6280	BOC-Office of Competitive Sourcing	3	0	1	0	0
4006	Office of Small Business Programs	12	2	11	0	0
6220	BOC-Cost Determination	1	1	0	0	0
6270	BOC-Office of Acquisition Services	1	2	1	1	0
6040	OASAM	3	0	2	0	0
6045	BOC -Worker Safety and Health	3	2	5	3	0
6100 and 6155	6100 is HRC-Office of the Director 6155 is Office of Administrative and Management Services	4	9	0	0	0
6840	Human Resources Center-Atlanta	0	0	1	0	0
6400	Office of Security and Emergency Management - Immediate Office	1	1	0	0	0
6051 and 6550	CPFR-Historian is code 6051 and 6550 if the Office of the Assistant Secretary for Admin. & Management-Library	6	0	7	0	0
4843 and 4844	Woman's Bureau-field office Atlanta is 4844 and 4843 is OPA field services-Atlanta	1	0	1	0	0
6760 and 6780	Civil Right Center (CRC) Dallas and Denver	2	0	5	0	0
6600	Information and Technology Center ¹¹	0	0	0	0	0
6070	Department Budget Center	46	3	21	0	0
6710	CRC-Boston	20	12	16	1	1
6700-6707	CRC -Office of Enforcement; Office of Mediation, Counseling, and Evaluation; Office of Compliance Assistance and Planning	5	3	5	1	0
Overall Totals		202	51	115	8	1

¹¹ The Departments Information and Technology Center stated that they were instructed to mark all unaccounted IT assets as disposed.

PAGE INTENTIONALLY LEFT BLANK

Exhibit 3**Agencies' Ability to Reconcile EPS IT Asset Information to EPMS**

Agency	Number of selected Items	No. of items for which data request was satisfied	No. of items for which data request was not satisfied	Percent of items for which data request was not satisfied
EBSA	9	2	7	78
ETA	20	10	10	50
MSHA	37	17	20	54
OASAM	45	0	45	100
OFCCP	28	0	28	100
OSHA	48	19	29	60
OWCP	22	0	22	100
WHD	22	0	22	100
Total	231	48	183	79

PAGE INTENTIONALLY LEFT BLANK

Exhibit 4**Reconciling Sensitive IT Assets from Floor to EPMS Inventory**

Agency	Number of Selected Items	Items Not Located in EPMS	Percent Missing
OASAM	30	1	3
EBSA	30	0	0
OHSA	30	0	0
MSHA	30	2	7
ETA	30	18	60
OWCP	25	4	16
OLMS	25	0	0
OFCCP	25	7	28
WHD	25	3	12
DITMS	20	3	15
Totals	270	38	14

PAGE INTENTIONALLY LEFT BLANK

Exhibit 5**Reconciling Sensitive IT Assets from EPMS to Floor**

Agency	Number of Selected Items	Number of Items Located	Percent of Items Located	Number of Items Not Located	Percent of Items Not Located
OASAM	38	8	21.05	30	78.95
OSHA	17	11	64.71	6	35.29
EBSA	11	9	81.82	2	18.18
OWCP	44	23	52.27	21	47.73
OLMS	10	7	70.00	3	30.00
OFCCP	42	19	45.24	23	54.76
MSHA	19	11	57.89	8	42.11
ETA	41	24	58.54	17	41.46
WHD	29	14	48.28	15	51.72
TOTAL	251	126	50.20	125	49.80

PAGE INTENTIONALLY LEFT BLANK

Exhibit 6

Missing EPMS IT Asset Data

Missing IT Asset Data	Number of Fields	Total Records	Total Number of Fields	Total Number of Blank Fields	Percent of Total Fields that are Blank
From EPMS Sample	33	29,106	960,498	205,064	21
From EPMS Overall	33	47,821	1,578,093	332,208	21

PAGE INTENTIONALLY LEFT BLANK

Appendices

PAGE INTENTIONALLY LEFT BLANK

Appendix A**Background**

Due to concerns over recent high-profile instances of laptop thefts and data breaches, the Federal government has been concerned about Federal agencies' ability to account for its sensitive IT assets. To push agencies to examine its risks and make substantial security improvements to address these concerns, in FY 2010 the Office of Management and Budget (OMB) developed an outcome-focused metric for information security performance for Federal agencies designed in part to ensure that Federal agencies are accountable for sensitive IT assets.

Securing our nation against cyber attacks has become one of the Nation's highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. Furthermore, for those external attacks that are successful, defenses must be capable of thwarting, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

A central tenet of the U.S. Comprehensive National Cyber-security Initiative is that "offense must inform defense." In other words, knowledge of actual attacks that have compromised systems provides the essential foundation on which to construct effective defenses. The U.S. Senate Homeland Security and Government Affairs Committee moved to make this same tenet central to the FISMA Federal Information Security Management Act in drafting requirements for FISMA 2009. The new proposed legislation calls upon Federal agencies to "Establish security control testing protocols that ensure that the information infrastructure of the agency, including contractor information systems operating on behalf of the agency, are effectively protected against known vulnerabilities, attacks, and exploitations."

Our audit objective was derived from the Consensus Audit Guidelines (CAG) and NIST-required, minimum security controls. CAG is a collaborative effort between industry and government to protect Federal and contractor information and information systems by identifying the most critical security controls to defending our nation's cyber systems from attacks. The CAG has identified critical controls specific to the inventory of IT devices and software. These controls correspond to NIST minimum security controls Configuration Management (CM) – 8 – Information System Component Inventory, and Certification and Accreditation (CA) – 7 – Continuous Monitoring.

In addition, OMB issued in a set of information security performance metrics that emphasize, among other items, the management of IT hardware and software inventories and includes the Agency's ability to accurately and completely identify and track its related Sensitive IT resources.

DLMS 2, Chapter 100, *Property Management*, assigns responsibilities for property management within DOL and sets forth guidance on the entire life cycle for property management from acquisition through retirement.

The maintenance and tracking of IT hardware and software inventory is a decentralized process throughout the Department. The Department's Information and Technology Center has indicated that it has responsibility to track and maintain IT hardware and software for those agencies housed on the Employee Computer Network¹². ITC and all other agencies are expected to track and maintain IT hardware and software using EPMS in accordance with DLMS 2 – Chapter 100 on *Property Management*. The only exception is the JC Data Center, which utilizes its own system — Job Corps Electronic Property Management System — to record and track data center property. All other JC inventory is maintained by ETA.

The EPS is used to procure IT hardware and software costing more than \$3,000. Per the Department's Purchase Card Program Handbook, "It is DOL policy to use the purchase cards whenever possible in lieu of purchase orders of \$3,000 or less." The Capitalized Asset Tracking and Reporting System are used to track DOL hardware and software assets valued at \$50,000 and above.

¹² Agencies on the ECN comprise the following: Bureau of International Labor Affairs (ILAB); Office of the Chief Financial Officer (OCFO); Office of Congressional & Intergovernmental Affairs (OCIA); Office of Disability Employment Policy (ODEP); Office of Public Affairs (OPA); Office of the Secretary (OSEC); Office of the Solicitor (SOL); Office of the Assistant Secretary for Administration & Management (OASAM); Office of the Assistant Secretary for Policy (OASP); Veterans' Employment & Training Services (VETS); Women's Bureau (WB); Administrative Review Board (ARB); Benefits Review Board (BRB) ; Office of Small Business Program (OSBP)

Appendix B**Objective, Scope, Methodology, and Criteria**

Objective

The audit objective was to answer the following question:

Can the Department account for its inventory of sensitive IT assets?

Scope

The audit covered procurement, inventory distribution and accountability, disposal of IT assets, reconciliation, and inventory update of sensitive IT hardware and software (property) during the period of October 1, 2006 through July 6, 2010 across the Department, comprising the following 10 program agencies:

- EBSA
- BLS
- ETA
- MSHA
- OSHA
- Office of Federal Contract Compliance Programs (OFCCP)
- Office of Labor-Management Standards (OLMS)
- OASAM
- Office of Workers' Compensation Programs (OWCP)
- Wage and Hour Division (WHD)

Our scope included the first five categories of sensitive property included in DLMS 2 Chapter 100, *Property Management*. These properties have personal appeal and subject to theft, security concerns or considered mission critical. They are as follows:

- (1) CPUs (All components of a computer would be classified as an accessory item for tracking purposes, e.g. a monitor is an accessory component of a computer)
- (2) BlackBerries/Personal Digital Assistants (PDA)
- (3) Laptops
- (4) Printers
- (5) Software licenses*

* Software only included commercial off-the-shelf software.

Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

A performance audit includes obtaining an understanding of internal controls considered significant to the audit objective and testing compliance with significant laws, regulations, and other requirements. Our work on internal controls included obtaining and reviewing policies and procedures and interviewing key personnel. We evaluated internal controls pertaining to assessing the reliability of related data maintained on EPS and the EPMS. We reviewed DOL's IT policies and procedures; reports on system controls and internal monitoring reports. We did not intend to form an opinion on the adequacy of internal controls overall, and we do not render such an opinion.

To achieve the audit's objective, we assessed the quality of sensitive IT asset data contained in the EPS and the EPMS by (1) performing analytical tests of data elements, (2) interviewing agency officials knowledgeable about data and system controls, (3) reviewing OIG and GAO reports on EPS and IT Inventories, (4) utilizing corroborating on-line EPMS records, (5) examining records, (6) verifying the existence of assets recorded in the EPMS, and (7) tracing selected assets to source documents. Based on these tests and assessments, we concluded the EPS data was sufficiently reliable to be used in meeting the audit objective, with the exceptions of classification of category code, the 204 occurrences of negative quantity ordered, and the 1,015 procurements with a unit price of zero dollars. We performed the following specific audit procedures for each major audit segment:

Procurement

We analyzed the procurements in the EPS with the category code 1 (unknown) and category code 4 (EIT) for the period between October 2006 through December 2009. We identified 2,406 procurements made by the 10 program agencies with descriptions that indicated sensitive IT properties, such as server, laptop, PDA/ blackberry, printer, and software. From these 2,406 procurements, we selected two stratified statistical samples as defined below that included 432 procurements using a 95 percent confidence level and a sampling precision of plus or minus 7 percent.

- For category code 1 procurements, we statistically sampled 270 IT procurements from the 1,423 unclassified procurements. .
- For category code 4 procurements, we statistically sampled 162 IT procurements from the 983 EIT procurements.

We compared these samples to inventory records to determine if the procurements were recorded on the inventory records.

Inventory Distribution and Accountability

We utilized the EPMS database provided by the Department to generate a universe for our analysis. We removed any records from the database that were outside the timeframe of the audit scope. Then we reviewed the universe and removed any records outside the scope of the audit type of items being reviewed (those being CPUs, BlackBerries/ PDAs) Laptops, Printers and Software Licenses). Finally we reviewed the universe for any records that were outside of the scope of the audit status (only items that are in-service are being examined); the auditors removed all records with status descriptions that were not "In-Service". Once this work was completed we examined the resultant universe in a spreadsheet and constructed charts with analysis, for instance the breakdown of blank fields across all of the data and an examination of the number of items that were unassigned broken down by Agency.

Reconciliations

To gain a better understanding of Sensitive IT assets for the EPS and the EPMS activities, we sampled procurements and inventories and performed appropriate data reliability procedures for our physical inventory testing at DOL's 10 program agencies to include (1) testing the existence of items in the database by observing the physical existence of items at DOL national office and IT equipment selected in our sample, and (2) testing the completeness of the EPMS database by performing a "floor-to-inventory" inspection at DOL and judgmentally selecting inventory items in our sample to determine if these items were maintained in EPMS inventory records.

In addition, we interviewed DOL agency officials, property management staff, and other DOL employees. We also interviewed DOL officials concerning the migration of EPMS. Additionally, we judgmentally selected items for on-site testing in the 10 program agencies by conducting a walk through of the agencies' offices and selecting sensitive IT assets from the floor to reconcile to the EPMS inventory.

Disposal

We interviewed OASAM officials to identify the existence of department-wide policies and procedures that govern how the program agencies are to dispose of IT assets. In addition, we extracted disposal activity from EPMS ranging from October 1, 2007 – June 1, 2010. We compared this activity to the activity shown in a disposal report provided by OASAM officials within the same date range to identify if there were any discrepancies. To identify whether or not a potential for an information security breach was present, we obtained copies of the I-2094 forms from OASAM by Cost Center to determine sensitive IT assets that were reported lost/missing/stolen during the 2010 recertification process.

Inventory Update

On January 5, 2010, the Assistant Secretary of OASAM required all program agencies to verify their respective inventories and update EPMS to record and track the assets. We reviewed the certifications as of July 8, 2010, and performed an analysis to confirm the validity of those agencies that certified their inventory as complete and accurate. In addition, we asked program agencies to confirm how they maintained their software licenses. Next, we performed analysis of the entire EPMS database from October 1, 2007 – July 6, 2010 to identify missing data and/or errors within the system. Using this same database, we sorted the data by program agency to identify how much of the database consisted of BLS information (the number of assets and costs associated) in lieu of them maintaining their inventory separately from the rest of the Department. We requested that BLS provide documentation that the Department granted it an exemption from maintaining its inventory in the Department's EPMS. Finally, we requested BLS to provide documentation that its separate inventory system, AMS, was categorized by risk, as required by FIPS 199.

The obvious and systemic control deficiencies we identified are the result of DOL's inventory system's lack of proper accountability of IT sensitive assets in all five phases of the inventory process — procurement, inventory distribution and accountability, disposal, reconciliation, and inventory update — and the Chief Information Officer's (CIO) lack of oversight. Without significant improvements in oversight, accountability, and inventory controls, the Department risks the potential of eroding the public's trust should an undetected information security breach occur.

Criteria

DLMS

- DLMS 2, Administration, Chapter 100, Property Management, dated May 2, 2005
- DLMS 6, Financial Management, Chapter 730, Management of Capitalized Assets, dated June 12, 2003
- DLMS 6, Financial Management, Chapter 750, Leases & Software Licenses, dated December 21, 2006
- DLMS 9, Information Management, Chapter 200, IT Capital Investment Management, dated March 31, 2004
- DLMS 9, Information Management, Chapter 300, Management & Accountability of Information Resources, dated August 12, 2003
- DLMS 9, Information Management, Chapter 400, Security, dated February 15, 2007
- DLMS 9, Information Management, Chapter 600, IT Accessibility Management, dated, March 25, 2005
- DLMS 9, Information Management, Chapter 1000, Software Management, dated August 12, 2003
- DLMS 9, Information Management, Chapter 1200, Safeguarding Sensitive Data Including Personally Identifiable Information, dated January 8, 2008

CAG

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software

NIST SP 800-53

- AC: Access Control
- CM: Configuration Management
- SA: System & Services Acquisition
- CA: Certification, Accreditation, and Security Assessments

NIST SP 800-88

- Guidelines for Media Sanitization

FIPS 199

- Standards for Security Categorization of Federal Information and Information Systems

DOL PII Breach Notification Policy

Joint Financial Management Improvement Program Inventory and Supplies Management (JFMIP)

- JFMIP-SR-OO-4 Property Management System Requirements

Department of Homeland Security Presidential Directive (HSPD)

- HSPD – 7: Critical Infrastructure Identification, Prioritization, and Protection

PAGE INTENTIONALLY LEFT BLANK

Appendix C**Acronyms and Abbreviations**

AMS	Asset Management System
APO	Accountable Property Officer
BLS	Bureau of Labor Statistics
BOC	Business Operation Center
CAG	Consensus Audit Guidelines
CIO	Chief Information Officer
CSH	Computer Security Handbook
CPU	Central Processing Unit
CRC	Civil Rights Center
DLMS	Department of Labor Manual Series
DOL	Department of Labor
DOLCSIRC	DOL Computer Security Incident Response Capability
EBSA	Employee Benefits Security Administration
EIT	Electronic and Information Technology
EPMS	E-Property Management System
EPS	E-Procurement System
ESA	Employment Standards Administration
ETA	Employment and Training Administration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Auditing Standards

HSPD	Department of Homeland Security Presidential Directive
ISO	Information Security Officer
IT	Information Technology
JC	Office of Job Corps
JFMIP	Joint Financial Management Improvement Program Inventory and Supplies Management
MIS	Management of Information Systems
MSHA	Mine Safety and Health Administration
NIST	National Institute of Standards and Technology
OAS	Office of Administrative Services
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OFCCP	Office of Federal Contract Compliance Programs
OIG	Office of Inspector General
OLMS	Office of Labor-Management Standards
OMB	Office of Management and Budget
OSEC	Office of the Secretary
OSHA	Occupational Safety and Health Administration
OWCP	Office of Workers' Compensation Programs
PDA	Personal Digital Assistants
PII	Personally Identifiable Information
SP	Special Publication
US-CERT	United States – Computer Emergency Readiness Team
WHD	Wage and Hour Division

Appendix D

OCIO Response to Draft Report

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

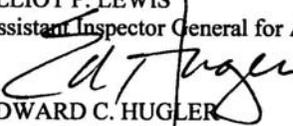


MAR 30 2011

MEMORANDUM FOR ELLIOT P. LEWIS

Assistant Inspector General for Audit

FROM:


EDWARD C. HUGLER
Deputy Assistant Secretary for
Administration and Management

SUBJECT:

Ineffective Accounting for Sensitive Information Technology
Hardware and Software Assets Placed DOL at Significant
Risk: Draft Report No. 23-11-001-07-001

This responds to the above-described draft report dated March 24, 2011. The stated audit objective was to determine the Department's ability to account for its inventory of sensitive Information Technology (IT) hardware and software.

This draft audit report was one of four delivered to the Department's Chief Information Officer (CIO) in the past few business days—all with due dates for management's reply set for March 29 or 30, 2011. As a result, management was afforded only a few business days for the preparation of final responses. Management acknowledges that we were contacted at the staff level and recently participated in meetings on a discussion draft of this report. However, for the most part, very little of the input offered—which was focused on balance and fairness—was adopted in the draft report. For completeness, we have captured the major topics of our input in the comments below.

At the outset, management acknowledges that there are deficiencies in the property management system and is prepared to take corrective action. However, the report contains erroneous assumptions that form a misleading portrayal of the issues and the severity of the associated risks:

- Use of the Term "Sensitive" IT Assets. All DOL IT assets are not "sensitive" and the use of this term is misused throughout the report. The security sensitivity of an IT asset is based on the type of data that is stored or processed on the asset as well as the function of the asset. The draft report does not explain if or how the security sensitivity of information stored or processed on IT assets was evaluated during the audit.
- No Acknowledgement that the E-Procurement System (EPS) Was Not Intended to be Part of DOL's E-Property Management System (EPMS), Page 3 and subsequent pages. Beginning with the section on "Procurement" on page 3, the draft report focuses on EPS as part of the Department's EPMS and on functions that EPS was never intended to

perform. Focus should be placed on the inventory “process and results,” which can be improved, rather than an automated procurement system that is performing within its design parameters. Notably, the report never acknowledges that EPS is performing as designed and continues the misleading notion that EPS should be something other than what it is—a system for procuring certain goods and services. It is not the function of EPS to account for all assets—nor can it do so. For example, DOL purchase card users have the ability to purchase IT assets up to \$3,000 without using EPS. Over \$2 million in such assets were acquired using purchase cards in FY 2010. This should be corrected in the final report.

In addition, page 11 of the draft report states that “[t]here was no electronic interconnection between EPS and EPMS.” The statement is factually correct, but there is no requirement that the systems be connected and electronic integration of the two systems is not part of the design. The statement implies the Department is required to have the systems connected and that integration of the two systems is the only acceptable way to account for the Department’s IT assets. This is an incorrect statement and should be corrected in the final report.

- **Lack of Relevance of EPS Errors to EPMS, Page 4.** Page 4 of the draft report provides and example of an EPS data input error by stating that a \$1 million procurement action was coded as \$77 million. However, the report fails to explain how an error in EPS is relevant to EPMS, a system not connected to EPS. It implies without explanation that the Department incorrectly procured goods or services worth \$1 million at a cost of \$77 million, which is not the case. Since EPS is not part of the Department’s inventory system, it is not clear how the coding error in EPS is relevant to the stand alone EPMS. OASAM has requested the background information on this finding so that it can be investigated to clarify the meaning of the error. It is quite possible that there is an error, but that a system user made a mistake in entering data which was later corrected.
- **Mischaracterization of a Significant Deficiency, Page 12.** The draft report states the DOL information security program has worsened as a result of the deficiencies identified in the audit and, with no analysis, concludes that the issues identified in the report meet the definition of a significant deficiency under FISMA. It is management’s view that the information provided does not warrant the classification of a significant deficiency.

Be assured that nothing in this response is intended to suggest that management does not take seriously the recommendations of the OIG. With the caveats outlined above, management accepts the spirit of the recommendations in the audit report and will take the following actions:

Recommendations

1. *Assess and take appropriate measures to ensure reports of lost, missing, or stolen sensitive IT assets have not resulted in loss of sensitive (PII) information in accordance with US-CERT and DOL Information Breach Policy and Procedures.*

Response: OASAM will review existing property systems for enhancements/modifications to ensure adequate controls for inventory accounting and reporting IT assets. This will include short-term measures and longer-term solutions. By the 4th quarter of FY 2012 OASAM will have an interim mitigation plan underway to improve the accountability of IT assets, pending a longer-term solution. After making a determination of the enhancements/modifications required, and contingent on funding availability, changes to the property management program will be implemented to improve property accountability. The review, development and implementation are expected to be complete within 18 – 24 months, or in the 3rd quarter of FY 2012.

2. Perform a full inventory of the Department's IT assets that is accurate and complete including an update of the information into a viable inventory management system.

Response: As part of the interim solution described above, OASAM will issue a call for a DOL agencies to conduct a full inventory of reportable personal property, including information technology assets, to be completed by the 4th quarter of FY 2012.

3. Consolidate all inventory systems throughout DOL to eliminate duplication, realize cost savings, and strengthen inventory and security controls over IT assets.

Response: This recommendation does not take into account that the Office of Job Corps maintains its own independent, contractor-operated system for property maintained at Job Corps centers. The more appropriate recommendation should be that the inventory process conforms with DLMS Chapter 2, Section 100, which provides that DOL will utilize an enterprise-wide property management system (EPMS) to record, track, and verify information pertaining to accountable property through decentralized oversight by the OASAM's Business Operations Center. The DLMS also states the "...policy applies to all DOL agencies and offices nationwide regarding accountability for tracking and maintaining current property records. The Job Corps Center property will be centrally managed by the Employment and Training Administration, Office of Job Corps."

OASAM will consolidate all inventory systems making EPMS the one authoritative source for asset inventory control and oversight, with the exception of the Job Corps Center inventory as required by DLMS Chapter 1, Section 100, by the 4th quarter of FY 2012.

4. Perform required reviews of program agencies' inventory practices and procedures to ensure full participation in the inventory process across the Department and compliance with Federal information system requirements.

Response: In accordance with the policy established by DLMS-9, Chapter 300, Paragraph 306 A (2), the Chief Information Officer will periodically review agencies' information resources accountability and inventory practices to ensure they meet all legal requirements.

5. Develop policies for disposal of sensitive IT assets that presently lack coherent policy.

Response: OASAM will issue updated policy guidance for the disposal of sensitive IT assets by the 4th quarter of FY 2011.

6. Integrate a reliable electronic procurement system with a viable inventory system along with the financial systems to ensure seamless interoperability

Response: This recommendation goes beyond the scope of the audit by recommending how to specifically remedy the issues identified in the report. While such an integrated solution may be desirable, it is inappropriate to limit management's options. The more appropriate recommendation should be to implement processes to ensure the Department can account for its assets in accordance with DOL policy.

With this in mind, the Department will continue to review and implement systems, policies and procedures that serve to integrate its electronic procurement, inventory management and financial management systems, in line with funding availability.

cc: T. Michael Kerr, Chief Information Officer
Al Stewart, Procurement Executive
Thomas Wiesner, Deputy Chief Information Officer

Appendix E

Acknowledgments

Key contributors to this report included Paul Kuscher, Paul Vaclavik, Tia Salmon, Carmen Wilson, Brian Devaney, Mitchell Goldberg, Lewis Leung, Victor Chan, and Benjamin Brady.

Additional support for this report was provided by Christine Allen, Ajit Buttar, Kevin Dolloson, Johanna Nathanson, and Steve Witherspoon.

PAGE INTENTIONALLY LEFT BLANK

TO REPORT FRAUD, WASTE OR ABUSE, PLEASE CONTACT:

Online: <http://www.oig.dol.gov/hotlineform.htm>

Email: hotline@oig.dol.gov

Telephone: 1-800-347-3756
202-693-6999

Fax: 202-693-7020

Address: Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, N.W.
Room S-5506
Washington, D.C. 20210