



governmentattic.org

"Rummaging in the government's attic"

Description of document: Seven (7) Department of Labor (DOL) Office of Inspector General (OIG) Audit Reports, 2007-2014

Requested date: 31-May-2016

Release date: 30-September-2019

Posted date: 02-December-2019

Source of document: FOIA Request,
Disclosure Officer
Office of Inspector General
U.S. Department of Labor
200 Constitution Ave., N.W., Room S-5506
Washington, DC 20210
Fax: (202) 693-7020

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



September 30, 2019

This is in final response to your Freedom of Information Act request addressed to this office for copies of reports for audit numbers 22-14-008-04-431, 23-07-005-11-001, 25-08-001-50-598, 23-14-011-07-727, 23-07-002-598, 23-13-004-07-001, 23-12-010-07-001, 23-13-006-07-001. Your request was received on May 31, 2016 and was assigned FOIA case number 216047.

The policy of the Inspector General is to make, to the extent possible, full disclosure of our identifiable records in accordance with the provisions of the Freedom of Information Act. Accordingly, I am enclosing a copy of all materials responsive to your request. However, certain information, which includes information technology audit processes and findings, and individual's identities have been redacted from the enclosed documents. All of the redactions made to the enclosed pages, unless otherwise marked, have been withheld under Exemption (b)(7)(e). The withheld information is subject to various FOIA exemptions, as discussed below.

Exemption (b)(7)(C) of the FOIA authorizes the withholding of names and details of personal information related to various individuals that is contained in audit reports which, if disclosed to the public, could reasonably be expected to constitute an unwarranted invasion of personal privacy. In this case, names and information that would reveal identities have been redacted on two reports pursuant to 5 U.S.C. 552(b)(7)(C).

Exemption (b) (7)(e) protects law enforcement information that would disclose techniques or procedures for audits and law enforcement investigations. In this case, specific details regarding techniques used to audit or protect highly sensitive information technology systems and multi system processes, vulnerabilities, and tools that the OIG uses for audit/investigative purposes have been redacted on the enclosed pages. In this case, information that reveals areas being audited, specific techniques used to uncover system vulnerabilities and technical details associated with system functions contained throughout the reports has been redacted. This information, if released could allow certain individuals, both external and internal, to illegally access or circumvent the system, and/or elude detection.

Although some reports are older, the same procedures and techniques apply to those complex information systems because the systems and business processes have not changed and therefore the sensitivity of the information and its protections under FOIA still apply.

Furthermore, one document, 25-08-001-50-598, an agency response to a Congressional Correspondence letter from Chairman Waxman in 2009 listing unimplemented audit recommendations was not located. The retention for Congressional Correspondence is 3 years. In addition, the FOIA case file (29017) which would have also contained a copy of the document was disposed of in accordance with NARA record retention schedule 4.2 Item 020.

Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You have the right to appeal this response within 90 days from the date of this letter. Should you decide to do this, your appeal must state, in writing, the grounds for appeal, together with any statement or arguments. Such an appeal should be addressed and directed to the Solicitor of Labor, citing OIG/FOIA No.216047, Room N-2428, 200 Constitution Avenue, N.W., Washington, D.C. 20210. Please refer to the Department of Labor regulations at 29 CFR 70.22 for further details on your appeal rights.

Should you need to discuss your request, feel free to contact this office at 202-693-5113 or the DOL FOIA Public Liaison, Thomas Hicks at 202-693-5427. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Finally, fees were not charged for this request. If you have any concerns regarding this letter, feel free to contact me at this office at 202-693-5113 and refer to FOIA case number 216047 on future inquiries. I hope you find this information helpful and thanks for your patience.

Sincerely,
Kimberly Pacheco
Kimberly Pacheco
Disclosure Officer

Enclosures
7 audit reports

U.S. Department of Labor

Office of Inspector General—Office of Audit

OFFICE OF WORKERS'
COMPENSATION PROGRAMS



SERVICE AUDITORS' REPORT ON THE INTEGRATED FEDERAL EMPLOYEES' COMPENSATION SYSTEM

AND

SERVICE AUDITORS' REPORT ON THE CENTRAL BILL PROCESSING SYSTEM

FOR THE PERIOD OCTOBER 1, 2013 TO MARCH 31, 2014

This report contains proprietary and other sensitive information. It is being provided solely for the internal use of recipients and should not be further distributed or disclosed without prior authorization from the U.S. Department of Labor, Office of Inspector General.

Date Issued: September 10, 2014
Report Number: 22-14-008-04-431

Table of Contents

INSPECTOR GENERAL'S REPORT	3
EXHIBITS.....	5
A. Service Auditors' Report on the Integrated Federal Employees' Compensation System performed by KPMG, LLP	
B. Service Auditors' Report on the Central Bill Processing System performed by Ethridge & Miller, PC	

THIS PAGE IS INTENTIONALLY LEFT BLANK

***Service Auditors' Report on the Integrated Federal Employees' Compensation System and
Service Auditors' Report on the Central Bill Processing System***

U.S. Department of Labor

Office of Inspector General
Washington, DC. 20210



Inspector General's Report

September 10, 2014

TO: FEDERAL AGENCIES WITH RESPONSIBILITIES FOR THE
FEDERAL EMPLOYEES' COMPENSATION ACT (FECA)
PROGRAM

Elliot P. Lewis

FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: Service Auditors' Reports on the Integrated Federal Employees'
Compensation System and the Central Bill Processing System,
Report No. 22-14-008-04-431

Attached are the Independent Service Auditors' Reports on the Integrated Federal Employees' Compensation System (iFECS) and the Xerox Business Services, LLC's (Xerox) Central Bill Processing System that were prepared to assist in the audit of your agency's annual financial statements. The U.S. Department of Labor (DOL), Office of Workers' Compensation Programs (OWCP), Division of Federal Employees' Compensation (DFEC) administers the FECA Special Benefit Fund (the Fund). DOL's Office of Inspector General (OIG) is responsible for auditing the Fund.

The OIG contracted with the independent certified public accounting firm of KPMG, LLP (KPMG) to perform an examination of the iFECS transaction processing for application and general controls for the period October 1, 2013, through March 31, 2014. The contract required KPMG to perform the examination in accordance with Generally Accepted Government Auditing Standards (GAGAS) and the American Institute of Certified Public Accountants' (AICPA) Statements on Standards for Attestation Engagement (SSAE) Number 16, Reports on the Controls at Service Organizations, as amended.

KPMG reported iFECS application and general controls, as described in the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved for the period October 1, 2013, through March 31, 2014.

OWCP contracted with the independent certified public accounting firm of Ethridge & Miller, PC (Ethridge & Miller) to perform an examination of Xerox's Central Bill Processing System controls for the period October 1, 2013, through March 31, 2014. The contract required the examination be performed in accordance with GAGAS and the AICPA's SSAE Number 16.

Ethridge & Miller reported Xerox's Central Bill Processing System controls, as described, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved for the period October 1, 2013, through March 31, 2014.

We reviewed the KPMG and Ethridge & Miller reports and related documentation and inquired of their representatives. Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to express, and we do not express, opinions on OWCP's description of controls, suitability of the design of those controls, and operating effectiveness of the controls tested. However, our review disclosed no instances where KPMG and Ethridge & Miller did not comply in all material respects with GAGAS and the AICPA's SSAE Number 16.

These reports contain proprietary and other sensitive information. They are being provided solely for the internal use of your office and should not be further distributed or disclosed without prior authorization from the OIG.

If you have any questions or comments, please send your comments via mail, facsimile, or e-mail to:

Joseph L. Donovan, Jr.
Audit Director
U.S. Department of Labor
Office of Inspector General
200 Constitution Ave., N.W., Room S-5512
Washington, D.C. 20210

Phone: (202) 693-5248
e-mail: donovan.joseph@oig.dol.gov

Attachments

Exhibits

THIS PAGE IS INTENTIONALLY LEFT BLANK

Exhibit A

THIS PAGE IS INTENTIONALLY LEFT BLANK

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

**OFFICE OF WORKERS' COMPENSATION PROGRAMS (OWCP)
DIVISION OF FEDERAL EMPLOYEES' COMPENSATION (DFEC)**

**INTEGRATED FEDERAL EMPLOYEES'
COMPENSATION SYSTEM
TRANSACTION PROCESSING, APPLICATION
AND GENERAL CONTROLS**

**REPORT ON DFEC'S DESCRIPTION OF ITS INTEGRATED
COMPENSATION SYSTEM AND THE SUITABILITY OF THE
DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS**

For the Period October 1, 2013 to March 31, 2014

Table of Contents

	<u>Page</u>
Section I: Independent Service Auditors' Report.....	1
Section II: Management's Assertion.....	5
Section III: Division of Federal Employees' Compensation Description of Controls	9
Overview of Operations	9
Relevant Aspects of the Control Environment	9
Control Environment.....	9
Risk Assessment.....	16
Information and Communication	16
Monitoring.....	18
User Organization Control Considerations	20
Control Objectives and Related Controls The Office of Workers' Compensation Programs, DFEC's control objectives, and The Office of the Assistant Secretary for Administration and Management (OASAM), ECN/DCN's control objectives, and their related controls are included in Section IV of this report, "Control Objectives, Related Controls, and Tests of Operating Effectiveness." Although the control objectives and related controls are included in Section IV, they are, nevertheless, an integral part of DFEC's and ECN/DCN's description of controls.	
Sub-Service Organizations	22
Section IV: Control Objectives, Related Controls, and Tests of Operating Effectiveness.....	25
Transaction Processing and Application Controls	25
Control Objective 1: Case/Claim Creation	25
Control Objective 2: Initial Eligibility.....	30
Control Objective 3: File Maintenance	32
Control Objective 4: Continuing Eligibility (Medical Evidence)	33
Control Objective 5: Continuing Eligibility (Earnings Information) ...	35
Control Objective 6: Accuracy of Compensation Payments	37
Control Objective 7: Permanent Impairment Schedule Awards.....	39
Control Objective 8: Medical Bill Payment Processing	40

General Controls	41
Control Objective 9: Entity-wide Security Program	41
Control Objective 10: Access Controls	45
Control Objective 11: Change Controls	50
Control Objective 12: System Software Modifications	53
Control Objective 13: Backup and Recovery	58
Control Objective 14: Computer Operations	60
 Section V: Other Information Provided by the Division of Federal Employees’	
Acronyms and Abbreviations	63



KPMG LLP
1676 International Drive
McLean, VA 22102

Section I: Independent Service Auditors' Report

Acting Director, Office of Workers' Compensation Programs, U.S. Department of Labor

Director, Division of Federal Employees' Compensation, U.S. Department of Labor

Deputy Chief Information Officer, Office of the Assistant Secretary for Administration and Management, U.S. Department of Labor

Office of Inspector General, U.S. Department of Labor

Scope

We have examined the U.S. Department of Labor (DOL), Office of Workers' Compensation Programs (OWCP), Division of Federal Employees' Compensation (DFEC) description of its transaction processing, application controls, and general computer controls for processing transactions for users of the Federal Employees' Compensation Act (FECA) Special Fund, Integrated Federal Employees' Compensation System (iFECS) throughout the period October 1, 2013 to March 31, 2014 (description) and the suitability of the design and the operating effectiveness of OWCP and The Office of the Assistant Secretary for Administration and Management (OASAM) controls to achieve the related control objectives stated in the description. OASAM is an independent service organization that provides computer processing services to OWCP. DOL's OWCP control description includes a description of the services provided by the Employee Computer Network/Departmental Computer Network (ECN/DCN) General Support System (GSS) used by DFEC to process transactions for its user entities, as well as relevant control objectives and controls of DFEC.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user organization controls and controls at the sub-service organizations contemplated in the design of DFEC's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or the operating effectiveness of such complementary user organization controls or controls at the sub-service organizations.

DFEC uses external service organizations (sub-service organizations). A list of these sub-service organizations is provided in Section III. The description in Sections III and IV includes only the control objectives and related controls of DFEC and excludes the control objectives and related controls of the sub-service organizations. Our examination did not extend to controls of the sub-service organizations.

Service organization's responsibilities

In Section II, DFEC and OASAM have provided their assertions about the fairness of the presentation of the description, and the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description. DFEC and OASAM are responsible for preparing the description and for the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks



that threaten the achievement of the control objectives; selecting and using suitable criteria; and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service auditors' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and applicable *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, the controls were suitably designed and the controls were operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2013 to March 31, 2014.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and the operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we considered necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization or sub-service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or sub-service organization may become inadequate or fail.



Opinion

In our opinion, in all material respects, based on the criteria described in DFEC's and OASAM's assertions, (1) the description fairly presents the DFEC iFECS system and OASAM ECN/DCN system used by DFEC for transaction processing, application controls, and general computer controls for processing of transactions for users of the FECA Special Fund that were designed and implemented throughout the period October 1, 2013 to March 31, 2014; (2) the controls related to the control objectives of DFEC and OASAM stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2013 to March 31, 2014; and (3) the controls of DFEC and OASAM that we tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description in Section IV were achieved, and operated effectively throughout the period October 1, 2013 to March 31, 2014.

Description of tests of controls

The specific controls and the nature, timing, extent, and results of the tests are listed in Section IV.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of DFEC, user entities of iFECS during some or all of the period October 1, 2013 to March 31, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

September 10, 2014

McLean, VA

THIS PAGE IS INTENTIONALLY LEFT BLANK

Section II: Management Assertion

U.S. Department of Labor

Office of Workers' Compensation Programs
Washington, D.C. 20210



September 10, 2014

Office of Workers' Compensation Programs
Division of Federal Employee Compensation
Office of the Assistant Secretary for
Administration and Management Employee
Computer Network/Departmental Computer
Network Assertion

We have prepared the description of the Office of Workers' Compensation Programs, Division of Federal Employees Compensation (DFEC) Integrated Federal Employees Compensation System (iFECS) and Office of the Assistant Secretary for Administration and Management (OASAM) Employee Computer Network/Departmental Computer Network (ECN/DCN) for user entities of the system during some or all of the period October 1, 2013 to March 31, 2014, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when obtaining an understanding of user entities' information and communication - systems relevant to financial reporting. We confirm, to the best of our knowledge and belief, that:

- a. The accompanying description in Sections III and IV, fairly presents the iFECS system and ECN/DCN system made available to user entities of the system during some or all of the October 1, 2013 to March 31, 2014 for processing their transactions in the iFECS system and ECN/DCN system.

DFEC and OASAM uses a number of different sub-service organizations for certain transaction processing:

Sub-Service Organization	Description of Services
Xerox Business Services, LLC (Xerox)	Processing of medical bills
Verizon Security Operations Center	Provides firewall and IDS services
Iron Mountain	Provides offsite storage for tape backups
Sprint Communications, Inc. and SunGard	Sprint Communications, Inc. partners with SunGard to provide managed data center services and to provide data center space, power, and a network connection

The description in Sections III and IV includes only the controls and related control objectives of iFECS and ECN/DCN and excludes the control objectives and related controls of the services listed above from the respective service organizations. The criteria we used in making this assertion were that the accompanying description:

- i. Presents how the systems made available to user entities was designed and implemented to process relevant transactions, including:
 1. The types of services provided, including, as appropriate, the classes of transactions processed;
 2. The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
 3. The related accounting records, supporting information, and specific accounts that were used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities;
 4. How the systems captured and addressed significant events and conditions, other than transactions;
 5. The process used to prepare reports or other information for user entities;
 6. Specified control objectives and controls designed to achieve those objectives;
 7. Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and

8. Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities transactions.
- ii. Does not omit or distort information relevant to the scope of the iFECS system and ECN/DCN system being described, while acknowledging that the description was prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the iFECS system and ECN/DCN system that each individual user entity may consider important in its own particular environment.
- b. The description includes relevant details of changes to the iFECS system and ECN/DCN system during the period covered by the descriptions.
 - c. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2013 to March, 31, 2014 to achieve those control objectives. The criteria we used in making this assertion were that
 - i. The risks that threatened achievement of the control objectives stated in the description were identified;
 - ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved;
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority; and
 - iv. Sub-service organizations applied the controls contemplated in the design of DFEC's and OASAM's controls.

Sincerely,

/Signed/

Gary A. Steinberg, Acting Director
Office of Workers' Compensation Programs
U.S. Department of Labor

/Signed/

Douglas C. Fitzgerald, Director
iFECS System Owner
Division of Federal Employees' Compensation
U.S. Department of Labor

/Signed/

Dawn Leaf
Chief Information Officer
Office of the Assistant Secretary for
Administration and Management
Office of the Chief Information Officer
U.S. Department of Labor

/Signed/

Louis Charlier
Director, Enterprise Services
ECN/DCN System Owner
Office of the Assistant Secretary for
Administration and Management
U.S. Department of Labor

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



Ethridge & Miller, PC
Building 1500
2255 Cumberland Parkway
Atlanta, GA 30339
USA
Tel: 770.437.0044
Fax: 770.437.8030

Independent Service Auditor's Report

To the Xerox Services IT Risk Governance Board

We have examined Xerox Business Services, LLC's (Xerox) description of its central bill processing system for the Department of Labor (DOL) to provide bill processing for the Office of Workers' Compensation Program (OWCP) throughout the period October 1, 2013 to March 31, 2014, (the "description") and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

In Section II of this report, Xerox has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Xerox is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion of the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material aspects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2013 to March 31, 2014.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion in Section II of this report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in Xerox' assertions in Section II of this report,

The description fairly presents Xerox' central bill processing system were designed and implemented throughout the period October 1, 2013 to March 31, 2014.

The controls related to the control objectives of Xerox stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2013 to March 31, 2014.

The controls of Xerox that we tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period October 1, 2013 to March 31, 2014.

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

The information included in Section V of this report is presented by Xerox to provide additional information to user organizations and is not a part of Xerox' description of controls placed in operation. The information in Section V has not been subjected to the procedures applied to the examination of the description of the controls related to the central bill processing system and, accordingly, we express no opinion on it.

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Xerox, user entities of Xerox' central bill processing system during some or all of the period October 1, 2013 to March 31, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

May 5, 2014

A handwritten signature in cursive script that reads "E. H. G. & Miller PC".

Atlanta, Georgia

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

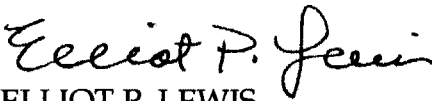
(b) (7)(E)

(b) (7)(E)



SEP 21 2007

MEMORANDUM FOR: PHILIP L. RONES
Deputy Commissioner
Bureau of Labor Statistics

FROM: 
ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: Status of Recommendations of the Audit Report:
Federal Information Security Management Act
Audit of the Bureau of Labor Statistics'
Producer Price Index System
Report No. 23-07-005-11-001

This memorandum transmits the results of the Office of Inspector General's (OIG) resolution follow-up work of audit report 23-06-013-11-001, issued September 29, 2006, to the Bureau of Labor Statistics (BLS). The follow-up work was performed to determine the resolution status of recommendations made in the subject report based on corrective actions completed by BLS and verified by the OIG as of August 23, 2007.

The September 2006 audit report contained three high-risk significant deficiencies with 12 corresponding recommendations and one medium-risk significant deficiency with 3 corresponding recommendations. Our resolution audit work has determined that all 15 recommendations are now closed. The resolution status of each recommendation is summarized for you in the attached table.

Please contact Keith E. Galayda, Director, Office of Information Technology Audits, at 202-693-5259, if you have any questions.

Attachment

cc: Cathy Kazanowski
Division Chief
BLS Division of Management Services (DMS)

Karen Windau
Division Chief
BLS Division of Producer Price Systems (DPPS)

Maureen Doherty
Acting Division Chief
BLS Division of Industrial Prices and Price Indexes (DIPPI)

Kristen Pollock
Audit Liaison
BLS DMS

Tom Wiesner
Deputy Chief Information Officer

Tonya Manning
Chief Information Security Officer

ATTACHMENT

**Resolution Status of Recommendations from BLS Audit Report:
Federal Information Security Management Act Audit
of the BLS Producer Price Index System**

ISSUE	R#	STATUS As of 9/29/2006	STATUS As of 8/23/2007
High-Risk #1 - Risk of Unauthorized Access to the System	1	1 - Resolved	1 - Closed
	2	2 - Resolved	2 - Closed
	3	3 - Resolved	3 - Closed
	4	4 - Resolved	4 - Closed
High-Risk #2 - Incomplete System Security Risk Identification	5	1 - Unresolved	1 - Closed
	6	2 - Unresolved	2 - Closed
	7	3 - Unresolved	3 - Closed
	8	4 - Resolved	4 - Closed
High-Risk #3 - Risk of Unauthorized System Changes	9	1 - Resolved	1 - Closed
	10	2 - Resolved	2 - Closed
	11	3 - Resolved	3 - Closed
	12	4 - Resolved	4 - Closed
Medium-Risk #1 - Inadequate Contingency Planning	13	1 - Unresolved	1 - Closed
	14	2 - Unresolved	2 - Closed
	15	3 - Resolved	3 - Closed

U.S. Department of Labor

Office of Inspector General—Office of Audit

**OFFICE OF THE CHIEF
INFORMATION OFFICER**

**EMPLOYMENT STANDARDS
ADMINISTRATION**



COMPUTER SECURITY INCIDENT INVOLVING E-MAIL DISTRIBUTION LIST TESTING

**NOTICE - THIS REPORT CONTAINS SENSITIVE
INFORMATION AND IS RESTRICTED TO OFFICIAL USE ONLY**

This report is being provided to agency officials solely for their review, comment, and appropriate action. It contains sensitive information, which should only be reviewed by individuals with a legitimate "need to know." Recipients of this report are not authorized to distribute or release it without the express permission of the Office of the Inspector General.

**Date Issued: March 30, 2007
Report Number: 23-07-002-50-598**

**U.S. Department of Labor
Office of Inspector General
Office of Audit**

BRIEFLY...

Highlights of Report Number: 23-07-002-50-598, to the Chief Information Officer and the Assistant Secretary for Employment Standards

WHY READ THE REPORT

The Office of the Chief Information Officer (OCIO) reported a Computer Security Incident (CSI) Report regarding an e-mail spoofing incident. E-mail spoofing is the modification of an e-mail message so a user receives an e-mail message that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into releasing sensitive information. The user believes the e-mail message is legitimate and it downloads malicious content to the computer.

The CSI Report identified the Employment Standards Administration (ESA) (b) (7)(C) Director as using his personal e-mail account to send an e-mail message impersonating the Employee's Computer Network Technical Announcement account as the sender.

E-mail spoofing is a violation of Department of Labor (DOL) *Appropriate Use of Information Technology* policy.

WHY OIG DID THE AUDIT

The Office of Inspector General (OIG) performed an audit to determine:

- Did the ESA (b) (7)(C) Director violate Department policy in testing the e-mail service with spoofed e-mail messages?

March 2007

COMPUTER SECURITY INCIDENT INVOLVING E-MAIL DISTRIBUTION LIST TESTING

WHAT OIG FOUND

We found that the ESA (b) (7)(C) Director's (Director) actions violated DOL policy when he took it upon himself to send spoofed e-mail messages to test the DOL e-mail service without being authorized to do so. However, he notified responsible agency officials in advance, the spoofed e-mail messages he sent caused no harm to the DOL e-mail service, and his actions resulted in the discovery of a security vulnerability related to DOL's e-mail system.

According to the Office of the Assistant Secretary for Administration and Management, steps have been taken to correct the vulnerability to prevent a similar incident from occurring. Regardless of the resultant positive impact, actions such as those taken by the Director result in computer security incidents and are unacceptable. DOL IT policy allows for a wide latitude of actions that agency officials can take in dealing with such an incident.

WHAT OIG RECOMMENDED

We have no recommendations as a result of this audit. The violation of departmental IT policy is a personnel matter; therefore, disciplinary action to be taken, if any, should be determined by the responsible agency.

Neither OCIO nor ESA provided comments to the draft report.

Table of Contents

	PAGE
EXECUTIVE SUMMARY	3
ASSISTANT INSPECTOR GENERAL’S REPORT	5
RESULTS	6
The Employment Standards Administration’s (b) (7)(C) Director violated Department policy but caused no harm	6
EXHIBIT	9
A. Timeline.....	11
APPENDICES	13
A. Background	15
B. Objective, Scope, Methodology, and Criteria	17
C. Acronyms and Abbreviations.....	19
D. Agency Response	21

[THIS PAGE INTENTIONALLY LEFT BLANK]

Executive Summary

The Office of Inspector General (OIG) performed an audit in response to a Computer Security Incident (CSI) Report from the Office of the Chief Information Officer (OCIO) regarding an e-mail spoofing¹ incident. The CSI Report identified the Employment Standards Administration (ESA) (b) (7)(C) Director as using his personal e-mail account to send an e-mail message impersonating the Employee's Computer Network (ECN) Technical Announcement account as the sender. Our objective was to determine:

- Did the ESA (b) (7)(C) Director violate Department policy in testing the e-mail service with spoofed e-mail messages?

Results

We found that the ESA (b) (7)(C) Director's (Director) actions violated Department of Labor (DOL) policy when he took it upon himself to send spoofed e-mail messages to test the DOL e-mail service without being authorized to do so. However, he notified responsible agency officials in advance, the spoofed e-mail messages he sent caused no harm to the DOL e-mail service, and his actions resulted in the discovery of a security vulnerability related to DOL's e-mail system. According to a senior level official in the Office of the Assistant Secretary for Administration and Management (OASAM), steps have been taken to correct the vulnerability to prevent a similar incident from occurring. Regardless of the resultant positive impact, actions such as those taken by the Director result in computer security incidents and are unacceptable. DOL IT policy allows for a wide latitude of actions that agency officials can take in dealing with such an incident.

Recommendations

We have no recommendations as a result of this audit. The violation of departmental IT policy is a personnel matter; therefore, disciplinary action to be taken, if any, should be determined by the responsible agency.

¹ E-mail spoofing is the modification of an e-mail message so a user receives an e-mail message that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into releasing sensitive information. The user believes the e-mail message is legitimate and it downloads malicious content to the computer. E-mail spoofing is a violation of DOL's *Appropriate Use of Information Technology* policy.

Agency Response

The CIO and Assistant Secretary for ESA provided no comments to the draft report.

OIG Conclusion

The OIG concludes the actions taken are a violation of departmental IT policy and is a personnel matter. Further because there are no recommendations made to the CIO or ESA, the audit is closed.

U.S. Department of Labor

Office of Inspector General
Washington, DC 20210



Assistant Inspector General's Report

Mr. Patrick Pizzella
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave., N.W.
Washington, D.C. 20210

Ms. Victoria A. Lipnic
Assistant Secretary for Employment Standards
U.S. Department of Labor
200 Constitution Ave., N.W.
Washington, D.C. 20210

The DOL-OIG conducted an audit of the events surrounding an e-mail spoofing incident that occurred in December 2005. We initiated the audit in response to a CSI Report from OCIO, which identified the Director as using his personal e-mail account to send an e-mail message impersonating the ECN Technical Announcement account as the sender. Our objective was to determine:

- Did the ESA ^{(b) (7)(C)} Director violate Department policy in testing the e-mail service with spoofed e-mail messages?

We conducted our audit in accordance with Generally Accepted Government Auditing Standards for performance audits. Our objective, scope, methodology, and criteria are detailed in Appendix B.

Results

Objective: Did the ESA (b) (7)(C) Director violate Department policy in testing the e-mail service with spoofed e-mail messages?

The Director violated Department policy when he took it upon himself to test the DOL e-mail service--by sending three spoofed e-mail messages--without being authorized to do so. He had previously expressed concern to the (b) (7)(E) that a virus e-mail message had gotten through the (b) (7)(E) mailing list as spam e-mail, and did not believe action was being taken to address this IT security issue. The Director notified (b) (7)(E) that he planned to run some tests from his home computer in the evening, and felt this was sufficient authorization for him to go forward. While the spoofed e-mail messages were not damaging to the DOL e-mail system, their discovery did necessitate an investigation by OASAM IT personnel to determine what had occurred. A positive result of the Director's actions was that he identified a security vulnerability in the DOL e-mail service that required corrective action.

The Director's unauthorized actions violated the 2005 ECN/Departmental Computer Network (DCN) Rules of Behavior, which state, in part: "... Any activity that violates Federal laws for information protection (e.g. hacking, spamming, etc.) is not permitted. . . ." Further, DOL Manual Series, (DLMS) 9, Chapter 1200, Section k., *Microcomputer and LAN Management, Sanctions for Misuse*, states: "Unauthorized or improper use of Government office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of improper use."

The following are details of the events that transpired surrounding the e-mail spoofing incident, and are also shown in a timeline at Exhibit A.

On November 29, 2005, the (b) (7)(E) mailing list received an e-mail message that contained a virus. Even though the e-mail anti-virus system caught and removed the virus, the e-mail message was able to get through as spam e-mail. As one of the e-mail message's recipients, the Director questioned the security policy of the distribution lists (b) (7)(E), but was told by (b) (7)(E) member that the e-mail message was directed at him and nothing was wrong with the distribution list.

On December 5, 2005, Director learned that the entire (b) (7)(E) mailing list had received the November 29th virus e-mail message. In following up on the matter with ESA (b) (7)(E) members, the Director said he would run some tests when he went home to determine what controls were not functioning properly, including whether ESA had configured something incorrectly during the (b) (7)(E).

From his home computer that evening, the Director created three e-mail messages to test whether controls on the distribution lists would allow spoofed e-mail messages to go through the DOL e-mail system. The recipients were as follows:

- The (b) (7)(E), which was where the earlier virus e-mail message had gotten through. If this was the only spoofed e-mail message to go through, it would indicate a problem with only that distribution group.
- The ESA distribution list. If this spoofed e-mail message and the one to the went through, it would indicate controls related to the were not configured correctly to handle e-mail spoofing.
- The ECN Technical Announcements distribution list. If this spoofed e-mail message went through, it would indicate controls related to the were not configured correctly to handle e-mail spoofing.

After sending the three spoofed e-mail messages, the Director signed onto his account and found that the messages were delivered, thereby showing vulnerabilities at all three levels: the, and. He then e-mailed to notify the team as to what he did, and instructed them to inform OASAM of his test and results. On the morning of December 6, 2006, an ESA e-mail administrator notified the ITC Help Desk of the e-mail spoofing incident and that there were security issues related to the system controls on the e-mail system.

The Director's actions caused no harm to the DOL e-mail service and resulted in the discovery of a security vulnerability related to DOL's e-mail system. However, in sending the spoofed e-mail messages, he violated departmental policy and necessitated an investigation by OASAM IT personnel to determine what had occurred.

Since this computer security incident occurred, corrective actions have been planned or taken. (b) (7)(E) Administrators resolved the issue on the and distribution lists, and a senior OASAM official told us that plans an to request that all agencies change to allow for. Regardless of the resultant positive impact, actions such as those taken by the Director result in computer security incidents and are unacceptable. DOL IT policy allows for a wide latitude of actions that agency officials can take in dealing with such an incident.

Recommendations

We have no recommendations as a result of this audit. The violation of departmental IT policy is a personnel matter; therefore, disciplinary action to be taken, if any, should be determined by the responsible agency.

Agency Response

The CIO and Assistant Secretary for ESA provided no comments to the draft report.

OIG Conclusion

The OIG concludes the actions taken are a violation of departmental IT policy and is a personnel matter. Further because there are no recommendations made to the CIO or ESA, the audit is closed.



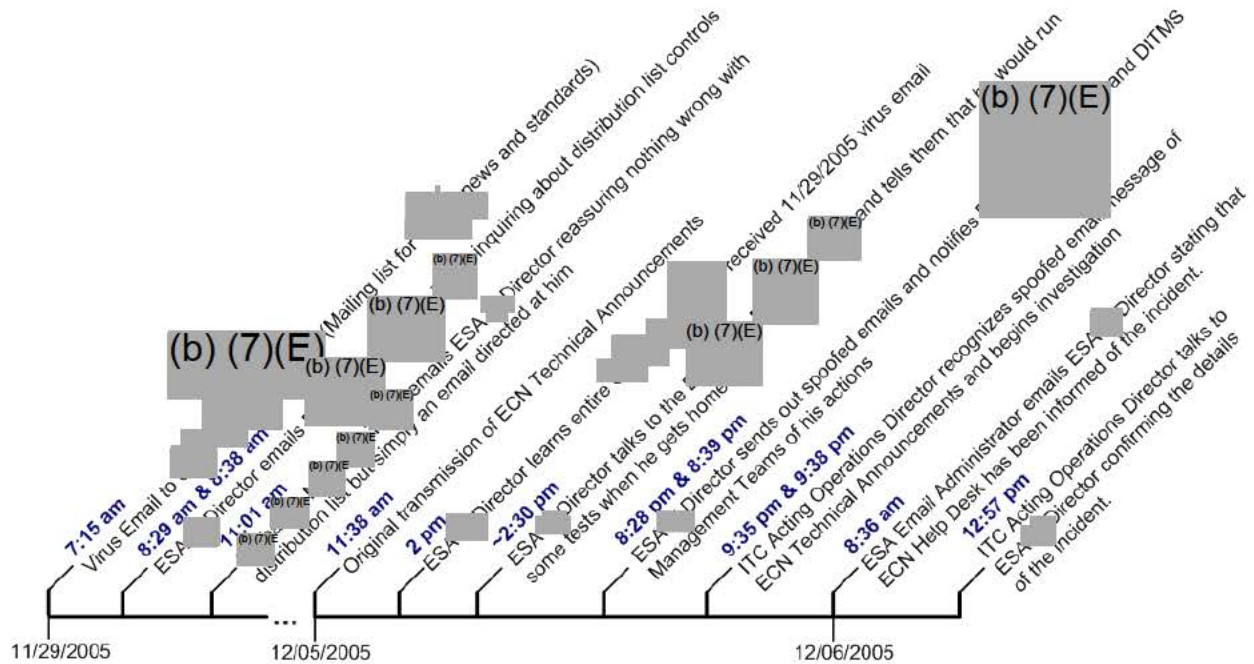
Elliot P. Lewis
March 28, 2006

Exhibit

[THIS PAGE INTENTIONALLY LEFT BLANK]

EXHIBIT A

Timeline



[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendices

[THIS PAGE INTENTIONALLY LEFT BLANK]

APPENDIX A

BACKGROUND

In February 2002, the Secretary launched a DOL initiative to unify the different e-mail systems within the Department. This initiative, known as the Common E-Mail System (CES), implemented an integrated e-mail system throughout DOL, unifying the Department's disparate e-mail systems to improve efficiency, effectiveness, and security. The CES provides additional services related to e-mail, such as group/mass mailings, spam blocking, security protections from spoofing, and unauthorized mass mailings.

OASAM's ITC is responsible for the management and implementation of ECN/DCN. ECN/DCN hosts CES and other services, and is the network providing connectivity and services to all DOL employees and agencies.

As part of the implementation, ITC formed (b) (7)(E), which incorporated knowledgeable staff from the various component agencies. (b) (7)(E) is to assist ITC by working with the agencies to incorporate their systems into CES by being a liaison and coordinating the agency efforts. ESA, a component agency of DOL, has several staff members on (b) (7)(E).

ESA maintains its own computers and networks that connect to OASAM's network. The group responsible for ESA computers and networks is the Division of IT Management Systems.

[THIS PAGE INTENTIONALLY LEFT BLANK]

APPENDIX B

OBJECTIVE, SCOPE, METHODOLOGY, AND CRITERIA

Objective

We received a CSI report from OCIO that dealt with a December 5, 2005, computer incident regarding the e-mail spoofing by the ESA [REDACTED] Director through the Department's e-mail distribution list service. The objective of our audit was to determine:

- Did the ESA [REDACTED] Director violate Department policy in testing the e-mail service with spoofed e-mail messages?

Scope

Our work on established internal controls included obtaining and reviewing policies and procedures, as well as interviewing key personnel to gain an understanding of the process and the controls involved in the computer incident. Our testing of internal controls focused only on the adequacy of the controls related to the incident and was not intended to form an opinion on the adequacy of internal controls overall, and we do not render such an opinion.

We validated the information in the CSI report, tracing the events that took place leading up to and following the e-mail spoofing incident, and evaluated related IT policy in place at that time. We performed our fieldwork from January 10, 2006, through April 26, 2006, in DOL's National Office located in Washington, D.C.

Methodology

We conducted interviews of Federal employees in OASAM, OCIO, and ESA, as well as contract staff, who were identified in the initial Security Incident Report, to validate the information in the incident report, including the affects of the incident on the Department's e-mail system. We developed a timeline using information from these interviews, and recreated, in a test environment, the steps involved to perform the e-mail spoofing. We also analyzed e-mail messages and relevant criteria, (e.g., OASAM and ESA Rules of Behavior, System Security documentation), including the last annual Computer Security Awareness Training, to evaluate current policy with regard to consequences of inappropriate behavior related to the use of IT.

We conducted the audit in accordance with Generally Accepted Government Auditing Standards for performance audits.

Criteria

DLMS 9, Chapter 1208 Appropriate Use of DOL IT (June 2000)
DOL Computer Security Awareness Training materials (completed Sept. 6, 2005)
OASAM IT System Rules of Behavior for ECN/DCN (June 1, 2005)
ESA IT Rules of Behavior (October 1, 2004)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

CES	Common E-Mail System
CSI	Computer Security Incident
DCN	Departmental Computer Network
DLMS	Department of Labor Management Series
DOL	Department of Labor
ECN	Employee Computer Network
EMT	Exchange Migration Team
ESA	Employment Standards Administration
IT	Information Technology
ITC	Information Technology Center
MS	Microsoft
OASAM	Office of Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OLMS	Office of Labor-Management Standards

[THIS PAGE INTENTIONALLY LEFT BLANK]

APPENDIX D

AGENCY RESPONSE TO DRAFT REPORT

No comments were provided by the CIO or the Assistant Secretary for ESA.



February 10, 2014

MEMORANDUM FOR: T. MICHAEL KERR
Chief Information Officer

A handwritten signature in blue ink that reads "Elliot P. Lewis".

FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: HR Works Implementation Review
Report Number: 23-14-011-07-727

HR Works is the Department of Labor (DOL) project migrating DOL's human resources (HR) systems (PeoplePower, PeopleTime, webPARs and Brio Portal/Query) to Department of the Treasury's (Treasury) Shared Service Center (SSC). We performed a review of the HR Works project to identify any concerns needing immediate attention. Our review covered the period December 11, 2013, through February 6, 2014, and encompassed DOL's functionality testing, security assessment, and project management.

As part of DOL's continuing efforts to comply with Office of Management and Budget (OMB) Memorandum 13-08, *Improving Financial Systems Through Shared Services*, DOL is migrating its HR systems to the Treasury's SSC. The purpose of shared services is to eliminate substantial cost overruns, simplify complex systems, and perform quick and easy updates, deployments, or needed improvements. Also, DOL considered its current HR systems no longer supportable, at risk of potential failure, and antiquated compared to current web-based SSC systems.

Treasury's SSC contains three parts: HR Connect, webTA, and Workforce Analytics. HR Connect will replace DOL's PeoplePower and DOL's WebPARS; webTA will replace DOL PeopleTime; and Workforce Analytics will replace Brio Query, DOL's HR Analytical and Reporting tool. The Department of Agriculture's National Finance Center (NFC) will continue to process DOL's payroll by using Treasury's SSC data feed.

RESULTS

During the time we conducted our review, DOL's testing of HR Connect, webTA, and Workforce Analytics was continuing and testing results were changing daily. The results reported here are based on the information provided to us by DOL during the period of our review. We understand additional Treasury documentation and testing results were part of the HR Works project, but were not provided to us.

We reviewed DOL's criteria for making the Go/No-Go decision, functionality testing results (scripted testing, user acceptance testing, and pilot testing), the security assessment, and project planning. The December 2013 scripted testing results did not specify if certain tests passed or failed. This scripted testing also omitted dates when the tests were performed and who performed them, creating a lack of accountability and integrity. For example, the pass/fail category for the scripted test results spreadsheet was blank. While the primary control documentation was absent of key information, DOL provided emails, other supplementary documentation, and discussions related to the testing approach and completion of these tests. However, resolution of identified defects and issues was not documented. Without clear, reliable, and current information on the results of its acceptance testing, DOL could accept unnecessary risks in its migration to Treasury's SSC. As a result, DOL may encounter payroll inaccuracies and the need for time-consuming and costly reconciliations.

This report provides a complete discussion of the results and their related recommendations from our review of DOL's criteria for making the Go/No-Go decision, functionality testing, security assessment, and project management.

A. Criteria for Making the Go/No-Go Decision

Go/No-Go Decision – Management should make a Go/No-Go decision based on predetermined criteria related to a system's readiness to go live. DOL established the following criteria for its Go/No-Go decision for HR Works.

- Personnel Action Request (PAR) processing
 - Goal: 100% (or understandable from analysis) PAR that have been transmitted from HR Connect to NFC are successfully applied at NFC
 - Method: HR Connect/end user reports
- Time and Attendance (T&A)
 - Goal: No more than 0.25 hour (15 minutes) difference in each time entry

- Method: webTA & PeopleTime timesheet comparison & FESI build file¹
- NFC Payroll
 - Goal: 0% (or understandable from analysis and test environment capabilities) gross pay deviation from both systems
 - Method: TIME and PAYE run in IDMS 62 using the webTA FESI build file

While it is a top priority to ensure all HR system components are working as intended, it is also of equal priority that personnel are fully trained in the use of the system. Training personnel on a new system's features and operation is vital to ensuring the system is used in the most efficient and effective manner and is a Go/No-Go decision criteria worth adding. DOL provided a status update on February 6, 2014, on the progress of personnel taking related LearningLink training and it showed a significant number of personnel have not completed or were not accounted for in scheduling training. However, personnel can also take related training through LaborNet (web portal); there was no mechanism in place to track and identify personnel taking training using this method. More importantly, we did not see criteria for how many employees need to be trained prior to migration in order to have a successful implementation. While DOL does not need to train all of its employees before moving to the new system, it does need to establish criteria for the number and types of employees that need to be trained.

We recommend that the CIO:

- 1. Include the completion status of training in its Go/No-Go criteria and decision.**

B. Functionality Testing Results

Scripted Testing – To determine if Treasury's SSC would meet DOL's operational expectations and requirements, we reviewed scripted testing results for PAR processing in HR Connect, the December 2013 operational testing scripts for webTA, and pilot testing results in comparison to the Go/No-Go decision criteria for reasonableness and completeness. Scripted testing is an automated testing of the system using a set of instructions to determine if the system functions as expected.

DOL provided the OIG a listing of tests that it had intended to perform in 31 distinct areas using 1,496 test steps for HR Connect's PAR processing. However, the list did not indicate if tests had passed or failed and did not provide

¹ FESI Codes contain data element information for the Front-End System Interface (FESI) files that agencies transmit to NFC.

comments explaining the status of the tests. In addition, the tester, date of test, and agency were also not indicated. Such documentation helps to ensure that the tests are performed, any problems identified are addressed, and the test results are appropriately considered in the Go/No-Go decision (see attachment 1 for an example).

DOL officials said Treasury and DOL performed scripted testing on HR Connect. In a January 29, 2014, email to OIG, a DOL official noted: at the conclusion of this testing, Treasury identified 15 defects (see attachment 2) that needed to be corrected and 16 enhancements (see attachment 3) that needed to be developed. DOL has informed us that the 15 defects have been resolved with continued testing with Treasury officials, but DOL has not been able to provide documentation of the corrective actions it has implemented. DOL planned to retest HR Connect starting February 3, 2014. The results of the February 3, 2014, testing were not provided and remain unknown to us.

On January 28, 2014, DOL provided the OIG its results from webTA testing conducted on January 25-26, 2014. Our review of these 36 tests showed the following (see attachment 4):

- 16 tests were listed as passed.
- 14 tests remained blank with no information as to the status of the test.
- 6 tests were listed as pending without including a pass or fail status.

On January 29, 2014, DOL provided the OIG a list of 230 tests it planned to perform for webTA testing. On this list, all 230 results were blank and no tests were listed as passed.

On February 5, 2014, DOL stated blanks for the scripted testing results indicated the test passed. If an error was identified, a description would have been included in the test results, according to DOL. However, our review of the documentation showed that the tester's name, date of test, and agency performing the test were also blank (see attachment 1). Due to this method of documenting test results, DOL could not provide verification of these tests. Without positive documentation that all tests were performed and all results (pass and fail) recorded, DOL is at higher risk of accepting a system which will not function as expected.

The testing of Workforce Analytics is dependent on both HR Connect and webTA data, which is retained in a reporting database and refreshed by NFC and Treasury. DOL further noted in a documented statement without specific testing results that no defects were identified. However, since Workforce Analytics testing was dependent on HR Connect and webTA data, it could not be fully completed until testing of HR Connect and webTA had been successfully completed.

Performing all scripted testing and clearly recording whether the tests passed or failed is essential to the integrity of DOL's Go/No-Go decision. DOL should ensure that all testing was completed and acceptable results were obtained prior to implementing the system.

User Acceptance Testing – DOL's user acceptance testing in December 2013 for webTA identified concerns, which if left uncorrected, would result in an ineffective system and a high level of user frustration. For example, holiday hours were not included in timesheet totals, employees were able to earn more than 24 credit hours, and employees could not report telework hours.

While DOL has provided emails acknowledging these concerns and actions taken, it has not demonstrated through evidence that it has corrected these issues.

Pilot Testing – DOL conducted a 536 person pilot, including personnel action requests (PAR) and position budget management (PBM) testing (gross pay and hours), which includes transactions to the NFC. We reviewed the testing performed on the pay periods (PP) 24 and 25 PARs. This testing included personnel actions such as step increases, name changes, promotions, reassignments, and annual ratings. Any PARs for the 536 users in PP 24 and 25 that would be performed in PeoplePower normally would also be performed in parallel in HR Connect. In PP 24 and 25, there were a total of 7 PARs for pilot users. From the pilot test of 7 transactions, the NFC applied status showed (see attachment 5 for further details):

- 5 as non-applicable (transaction was not completed nor sent to NFC)
- 1 as pending
- 1 as verified NFC match response

DOL was originally going to perform webTA pilot testing in PP 19. The test data was loaded into the system, but due to the government shutdown, the pilot testing was not performed until PP 24 and 25. For PP 24, 492 webTA timecards were sent to NFC for processing:

- 27 were rejected
- 414 matched gross pay, requiring no further reconciliation
- 37 required further reconciliation due to personnel experiencing a change in per hour pay rate from PP 19 test data to PP 24 production data.

For PP 25, 445 webTA timecards were sent to NFC for processing:

- 24 were rejected
- 368 matched gross pay, requiring no further reconciliation
- 51 required further reconciliation due personnel experienced a change in per hour pay rate from PP 19 test data to PP 25 production data.

DOL and Treasury used (b) (7)(E) to correct identified problems. Regression testing is the process of testing changes to computer programs to make sure that the older programming still works with the new changes. Typically, before a new version of a software product is released, the old test cases are run against the new version to make sure that all the old capabilities still work. The reason they might not work is because changing or adding new code(s) to a program can easily introduce errors into the program. DOL was continuing to perform (b) (7)(E) until satisfied that identified problems have been fixed.

Although DOL had defined the criteria for its Go/No-Go decision, the DOL provided scripted tests did not contain assigned accountability or specific pass/fail results. User acceptance testing did not document resolution of identified testing issues. The pilot testing did not provide conclusive pass/fail results with some of the individual tests performed remaining with unconfirmed results. Such tests should clearly identify each test it would use to evaluate the criteria and should have clearly defined how the criteria would be met. Test results used in Go/No-Go decisions should be traceable to when actual tests were performed and by whom.

We recommend that the CIO:

- 2. Ensure that all operational and user acceptance tests are completed as planned and all issues identified during testing have been adequately addressed before the new system is implemented.**

C. Security Assessment

A security assessment using appropriate assessment procedures determines the extent controls were implemented correctly, operating as intended, and producing their desired outcomes.

Our review included DOL's HR Connect Documentation Review Summary and Treasury's ATO's signature pages for HR Connect, webTA and Workforce Analytics. OIG reviewed the ATO signature pages and all pages contained current and valid approved authorizations from Treasury.

DOL's HR Connect Documentation Review Summary

DOL reviewed the HR Connect System Certification and Accreditation (C&A) Package on September 21-22, 2012. The HR Connect System C&A package contained the data risk assessment of the required system security controls. This assessment included, among other things, consideration of the system security categorization. System security categorization applies to both information and information systems. Security categories are based on potential impact to an

organization if certain events occur that would jeopardize the information and information systems needed by the organization. Security categories should be used in conjunction with vulnerability and threat information when assessing risks. To effectively protect information, the System Security Plan (SSP) must ensure management, operational, and technical controls prescribed for an information system, are in place and are designed to protect the confidentiality, integrity, and availability of the system and its information.

In its September 25, 2012, summary review report, DOL documented five concerns and five recommendations, with one concern being critical to DOL's migration to Treasury's SSC. That concern and related recommendation is explained in an excerpt from the HR Connect Summary Review document:

1) Concern –

(b) (7)(E)

Recommendation –

(b) (7)(E)

DOL also noted four other concerns in its summary report that involved:

[REDACTED]

Each concern provided a recommendation for future resolution. However, DOL did not provide evidence in the form of documentation that indicated each of the above concerns and recommendations were appropriately mitigated.

² A loss of confidentiality is the unauthorized disclosure of information.

³ A loss of integrity is the unauthorized modification or destruction of information.

⁴ A loss of availability is the disruption of access to or use of information or an information system.

We recommend the CIO:

- 3. Provide documentation that demonstrates corrective actions to resolve and close all DOL identified security concerns and recommendations have been taken.**

D. Project Management

The Project Management Plan for HR Works Version 5.0, dated October 2013, is the document DOL developed during the planning phase to define and communicate its strategy and approach. It also assigns accountability to ensure that the outcome is as expected. We reviewed this document to ensure the project team addressed key aspects of the effort, such as project description, organization responsibilities, deliverables, goals, scope, objectives, key stakeholders, change control, project schedule and resources, managerial and technical process plans, and other elements intended to minimize implementation risks. Our review noted the project management documentation contained those key aspects and provided information to address each area. We identified no areas of concern needing management's attention.

DOL officials have stated work on the HR Works project is being performed 24 hours per day, 7 days per week. Despite this effort, the project's Go/No-Go Decision date has slipped 22 days and the Go Live target completion date slipped 72 days. DOL stated that these delays were caused by the government shutdown in October for 2013. DOL stated that it had held discussions with Treasury to ensure shutdown delays could be appropriately managed (See attachment 6 for these key milestones and replanned schedule due to the 2013 government shutdown). DOL now anticipates that it will migrate to Treasury's SSC in PP 3 (February 9 – 22, 2014).

Conclusion

As DOL moves forward with HR Works, we have identified additional actions that will help DOL ensure that it is implemented as intended. DOL needs to ensure that it has evidence all planned functional testing has been completed and resulted in confirmation the Treasury SSC applications will work as intended. Ensuring DOL personnel receive and complete the necessary training on use of the system's components is equally important. Without sufficient supporting documentation, we cannot say the system is not ready to go but we also cannot say that it is ready to go. If DOL does not ensure that these items are validated prior to implementation, unpredictable payroll inaccuracies could occur that would require time consuming and costly reconciliations.

We limited our review to the procedures described above and our analysis relied on documentation provided by DOL. We did not verify the information contained

within this documentation. Had we performed additional procedures, other matters may have come to our attention that we would have reported to you.

We met with your staff to discuss the results of our review and the contents of this report. We considered the information and feedback obtained during those meetings in preparing this report. We request management's written response to the report and recommendations within 5 business days from the date of the report.

We extend our appreciation to OCIO officials and staff for their assistance and cooperation during our review.

Attachments

cc: Ed Hugler
Dawn Leaf
Tonya Manning

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

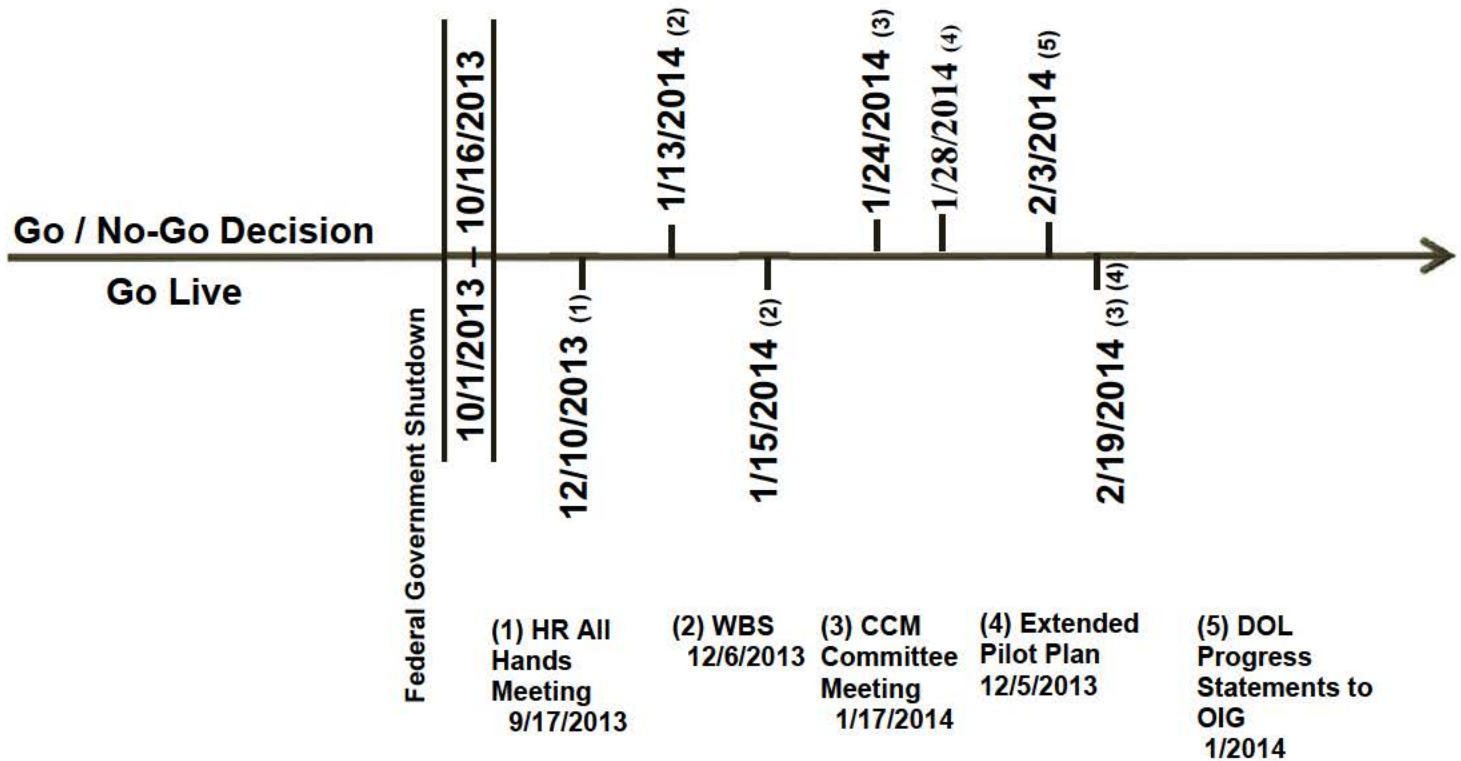
(b) (7)(E)

(b) (7)(E)

HR Works Migration Project

Government Shutdown Impacts Milestones:

DOL and Treasury negotiated new start and completion dates





OCT 10 2012

MEMORANDUM FOR: T. MICHAEL KERR
Assistant Secretary
for Administration and Management

A handwritten signature in black ink, reading "Elliot P. Lewis".

FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: Departmental eRecruit/DOORS System Testing
Report Number: 23-13-004-07-001

As part of our Federal Information Security Management Act audit work and other information technology (IT) security audit work completed for Fiscal Year 2012, we contracted with KPMG LLP (KPMG) to perform vulnerability assessments and testing of IT security controls for the Office of the Assistant Secretary for Administration and Management's (OASAM) e-Recruit/DOL Online Opportunity Recruitment System (e-Recruit/DOORS). Based on KPMG's work, we provided OASAM the 10 attached Notifications of Findings (NoF) for deficiencies identified in the following 7 security control areas: access controls, configuration management, contingency planning, risk management, security assessment and authorization, risk management, and third party oversight.

Overall, these deficiencies decrease the effectiveness of OASAM's security program and the control structure of e-Recruit/DOORS. Moreover, the deficiencies in third-party oversight, access controls, and contingency planning, could result in a loss of confidentiality, integrity, and availability of OASAM's information. For these reasons, and in consideration of the sensitivity of applicant data, we determined these deficiencies as a whole amount to a significant deficiency.

Unidentified vulnerabilities could be present since only a limited vulnerability scan was performed due to restrictions from the third party. As a result, we could not determine if the implemented controls were properly designed, in place, and implemented to prevent and detect unauthorized access within the eRecruit/DOORS. These deficiencies and unknown vulnerabilities increase the risk that there could be a breach of confidentiality, integrity, and availability of job applicant data within eRecruit/DOORS.

We recommend the Assistant Secretary:

1.



2.



3.



4. For all deficiencies identified in the 10 NoFs, create a Plan of Actions and Milestones describing mitigation strategies and corrective actions.

Please provide your response to each by October 31, 2013, describing your agency's planned corrective actions and anticipated dates of completion.

This report contains sensitive information and is restricted to official use. It is being provided to agency officials solely for their review, comment, and appropriate action. It contains sensitive information which should only be reviewed by individuals with a legitimate "need to know." Recipients of this report are not authorized to distribute or release it without the express permission of the OIG.

If you have any question, please contact Keith Galayda, Audit Director, at (202) 693-5259.

Attachment

cc: Edward Hugler
Tonya Manning

Attachment A

Summary of OASAM e-Recruit/DOL Online Opportunity Recruitment System (DOORS) Notifications of Findings*

Number	Control Family	NoF Title	Description
1		OASAM-ERD-01-	
2		OASAM-ERD-02-	
3		OASAM-ERD-03-	
4		OASAM-ERD-04-	
5		OASAM-ERD-05-	
6		OASAM-ERD-06-	
7		OASAM-ERD-07-	
8		OASAM-ERD-08-	
9		OASAM-ERD-09-	
10		OASAM-ERD-10-	

*For each above listing, a detailed Notification of Findings is attached.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)
System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)
Finding Number: OASAM-ERD-01-[REDACTED]
Date Provided to Management: September 15, 2012
Date Response Due: September 21, 2012
Title: [REDACTED]

CONDITION:

[REDACTED]
We inspected [REDACTED]
[REDACTED]

[REDACTED]
We determined that eRecruit/DOORS had not been defined or documented eRecruit/DOORS' [REDACTED]
[REDACTED]

Further, we inspected [REDACTED]
[REDACTED]

[REDACTED]
We inspected the Department of Labor (DOL) [REDACTED]
[REDACTED]

However, we were informed by the eRecruit/DOORS Data Administrator and the Project Manager that a compensating control, although not documented, is that eRecruit/DOORS [REDACTED]
[REDACTED]

Finally, we inspected documented Plans of Actions and Milestones (POA&Ms) for the above and determined that the above deficiencies were not previously identified by management.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

CAUSE:

We were informed by eRecruit/DOORS Project Manager and System Administrator that [REDACTED]

We were further informed that [REDACTED]

Finally, we were further informed that [REDACTED]

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 1, Version 1.0, dated August 2011, states in [REDACTED]
page 2 that:

Also the DOL CSH Edition 4.0, Volume 1, Version 1.0, dated August 2011, states in [REDACTED]
that:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

[REDACTED]

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3

[REDACTED]

Also, NIST SP 800-53, Rev.3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control

[REDACTED]

EFFECT:

Without effective controls in place to

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] may result in the unauthorized use, disclosure, or modification of job applicant data.

Finally, by not

[REDACTED]

the agency creates the risk that:

[REDACTED]

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

[REDACTED]

The DOORS team has taken immediate actions and [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)

System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)

Finding Number: OASAM-ERD-02-[REDACTED]

Date Provided to Management: September 15, 2012

Date Response Due: September 21, 2012

Title: [REDACTED]

CONDITION:

During our FY 2012 audit, we inspected and inquired and determined that eRecruit/DOORS [REDACTED]
[REDACTED]

Also, inspected documented Plans of Actions and Milestones (POA&Ms) and noted that the above deficiencies were not previously identified by management. Finally, we were informed by the eRecruit/DOORS Data Administrator and the Project Manager that and no compensating controls were in place.

CAUSE:

We were informed by eRecruit/DOORS Data Administrator and the Project Manager that control [REDACTED] were not documented as the security requirement was not formally implemented.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 1, Version 1.0, dated August 2011 states in [REDACTED]
[REDACTED]

NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in [REDACTED]
[REDACTED]

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

EFFECT:

Without adequate implementation of controls that [REDACTED]
[REDACTED] here is an increased risk that [REDACTED]
[REDACTED]

Further, [REDACTED]
[REDACTED] and could threaten the integrity of
eRecruit/DOORS application and job applicant data.

[REDACTED]

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

[Redacted Management Response]

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)
System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)
Finding Number: OASAM-ERD-03-CA.05
Date Provided to Management: September 15, 2012
Date Response Due: September 21, 2012
Title: Plan of Actions and Milestones (POA&Ms) were not Updated on a Timely Basis

CONDITION:

During our FY 2012 audit, we inspected the eRecruit/DOORS Detailed POA&M Report and determined that:

- 14 of the 21 POA&Ms identified as “delayed” listed the delay reason as “other” without rationale
- All 22 POA&Ms had targeted weakness and milestone completion dates that were not current and updated in Cyber Security Assessment and Management (CSAM) tool at the frequency required by DOL.

Further, we inspected the Quarter 2 Office of the Chief Information Officer (OCIO) POA&M Report Card and determined that they also identified that eRecruit/DOORS were not maintaining and updating milestone completion dates.

CAUSE:

We were informed by the eRecruit/DOORS Data Administrator and the Project Manager that due to conflicting priorities, POA&Ms were not updated at the DOL defined frequency.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 4, Version 1.0, dated August 2011, states in 3.1.5 Update the Security Plan of Action and Milestones, page 19-20, that:

DOL's required minimum standards on POA&M management are as follows:

- 1. Agency personnel must develop a POA&M for each information system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the system's security controls and to reduce or eliminate known vulnerabilities in the system.*
- 2. All known weaknesses within DOL information systems are recorded as POA&Ms for the information system as they are identified regardless of the activity in which the weakness was discovered.*

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

3. POA&M remediation must be independently validated using control assessment procedures outlined in the agency SCIP and/or concurrency by OIG.

4. The agency must review and update as appropriate existing POA&M information frequently but no less than quarterly to ensure POA&M information is current and addresses findings identified from security assessments, security impact analyses, and continuous monitoring activities. It is recommended that they be reviewed by the ISO and system owner with greater frequency to ensure that resolutions remain on budget and on schedule.

National Institute of Standards and Technology (NIST) Special Publication(SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control CA-5, Plan of Action and Milestones, that:

The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

EFFECT:

By not properly tracking the correct status of security weaknesses and including them in the POA&M process, OASAM management may not be adequately aware of the security weaknesses, an awareness that is paramount to protecting the e-Recruit/DOORS system and data. In addition, OASAM management may not be allocating the appropriate resources necessary to mitigate the current weaknesses relevant to the e-Recruit/DOORS production environment.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM management concurs with the NOF.

Since discussions with the OIG the DOORS team has taken corrective actions to resolve this NOF. Specifically, 19 out of 22 weaknesses have been addressed and are now closed in CSAM. For the remaining three (3) POA&Ms, the milestone completion dates are now current. OASAM considers this NOF closed and is prepared for the OIG to perform validation testing.

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)
System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)
Finding Number: OASAM-ERD-04-CA.07
Date Provided to Management: September 15, 2012
Date Response Due: September 21, 2012
Title: Deficiency around the Annual Security Self Assessment

CONDITION:

During our FY 2012 audit, we inspected the system security plan and inquired with management to determine that specific eRecruit/DOORS responsibilities were not documented under the controls listed as Hybrid.

We inspected the Security Self Assessment (SSA) in the Cyber Security Assessment and Management (CSAM) Tool and determined that the 14 hybrid control areas in scope for the FY2012 SSA did not contain additional testing or documentation (artifacts) covering the portion of the control under eRecruit/DOORS' responsibility.

Finally, inspected documented Plans of Actions and Milestones (POA&Ms) and determined that the above deficiencies were not previously identified by management.

CAUSE:

We were informed by the eRecruit/DOORS Project Manager and Data Administrator that specific control responsibilities were not documented and therefore testing over the hybrid controls were not supplemented with testing over OASAM's portion of the controls.

Further, we were informed that the Security Assessment Report provided by the third party was the only the basis of the SSA used in FY2012 as they were not aware this was not sufficient.

CRITERIA:

National Institute of Standards and Technology (NIST) Special Publication(SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control CA-7, Continuous Monitoring, that:

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

- *Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.*

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

The DOL Computer Security Handbook, Edition 4.0, Volume 4, Version 1.0, dated August 2011, states in 3.1.3 Assess Security Controls, page 15-16, that:

DOL's required minimum standards on conducting security assessments are as follows:

- *' DOL agencies must:*
 - (a) Develop a security assessment plan (SAP) that describes the scope of the assessment including:*
 - *Security controls and control enhancements under assessment*
 - *Assessment procedures to be used to determine security control effectiveness*
 - *Assessment environment, assessment team, and assessment roles and responsibilities*
 - (b) Assess the security controls in the information system at least once during the security authorization period to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements for the system. The frequency of testing per control may be more frequent depending upon the agency defined continuous monitoring plan or defined by OCIO Security.*
- *Agencies must ensure that the SCA results are documented in accordance with guidance provided by OCIO security using the Departmental approved methods and templates.*

EFFECT:

Without performing a security evaluation of the controls under OASAM's responsibility, it is unknown whether the controls are operating as intended. Performing such an evaluation provides knowledge and assurance that controls are functioning, and management is adequately aware of the security weaknesses.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM Management partially concurs with the NOF.

OASAM does not fully concur with the Cause. DOL has published the CSAM User Guide that defines expectations with documenting controls that are considered hybrid or fully inherited. Further guidance was emphasized in the *OASAM NIST SP 800-53 Revision 3 and FY12 Security Self-Assessment Implementation Plan* (dated February 2012) that was distributed to all OASAM system owners for the FY12 SSA process.

Where applicable and not already addressed in the DOL CSAM User Guide, the DOORS team will create and document procedures to address the hybrid controls – to include the responsibilities of all parties – and ensure the controls are properly tested in accordance with DOL policies. In addition, the DOORS team will take corrective actions in FY2013, by creating and documenting a Plan of Action and Milestones (POA&M). Specific dates will be included after negotiations with the DOORS vendor.

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)
System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)
Finding Number: OASAM-ERD-05-[REDACTED]
Date Provided to Management: September 15, 2012
Date Response Due: September 21, 2012
Title: [REDACTED]

CONDITION:

During our FY 2012 audit, we obtained and inspected the [REDACTED] -- After Action
[REDACTED]

Finally, we inspected documented Plans of Actions and Milestones (POA&Ms) and determined that the above deficiency was not previously identified by management.

CAUSE:

We were informed by the eRecruit/DOORS Data Administrator that the requirement for performing Training, Testing, and Exercises (TT&E) on an annual basis was not documented and tracked. We were further informed that the annual TT&E was not prioritized and was pushed back when other priorities were established.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 6, Version 1.0, dated August 2011, states in 3.2.1 Test Contingency Plan, page 13-14, that:

DOL's required minimum standards on contingency plan testing are as follows:

- 1. The contingency plan must be tested at least annually using agency-defined tests and exercises to determine the plan's effectiveness and the agency's readiness to execute the plan.*
- 2. The Agency tests and/or exercises the contingency plan for the information system at least annually for Moderate and High impact systems and at least every three years for Low impact systems. At a minimum functional exercises must be conducted for Moderate and High impact systems and classroom / tabletop exercises for Low impact systems to determine the plan's effectiveness and the agency's readiness to execute the plan.*
- 3. The Agency reviews the contingency plan test/exercise results and initiates corrective actions.*

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

4. *The results of contingency plan testing must be used to identify and remediate potential weaknesses.*
5. *The appropriate personnel shall review the contingency plan tests results, which must be documented in the contingency plan, and initiate corrective actions.*

National Institute of Standards and Technology (NIST) Special Publication(SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control CP-4, Contingency Plan Testing and Exercises, that;

The organization:

- a. *Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and*
- b. *Reviews the contingency plan test/exercise results and initiates corrective actions.*

NIST SP 800-34, Revision 1, Contingency Planning Guide for Information Technology System, dated May 2010, states:

Information System Contingency Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures.

EFFECT:

Without having tested the contingency plan, the deficiencies in the individual recovery may not be identified and addressed. As a result, in the event of a disaster the e-Recruit/DOORS System may not be adequate to continue tracking employment offers, providing employment opportunities, and hiring requirements.

Also, failure to adequately incorporate staff in testing and training of their Contingency Plan roles and responsibilities increases the risk of system recovery delays due to poor coordination or understanding of responsibilities.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM management partially concurs with the NOF as conditional elements identified herein have had corrective actions taken.

There are two (2) annual Contingency Plan (CP) testing activities: 1) a test conducted by the DOORS vendor; and 2) a separate notification drill conducted by the DOORS team. However, due to competing priorities, the DOORS team had not conducted a notification drill since March 29, 2011. Subsequently, the DOORS team ran a notification drill on September 10-11, 2012 and uploaded the test results and DOORS the CP points of contacts in CSAM.

The DOORS vendor performed their CP test in September 20, 2011 and provided the test results, which were uploaded and available in CSAM. OASAM considers the completion of the DOORS CP testing activities provided closure for the lack of CP testing being completed.

OASAM management agrees that proper tracking of CP testing completion was lacking. OASAM will take proactive actions to ensure the DOORS team conducts and tracks the necessary CP tests on an annual basis.

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

**Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012**

Office: Office of the Assistant Secretary for Administration and Management (OASAM)

System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)

Finding Number: OASAM-ERD-06-[REDACTED]

Date Provided to Management: September 15, 2012

Date Response Due: September 21, 2012

Title: [REDACTED]

CONDITION:

We obtained and inspected the system generated list of all users and determined that [REDACTED]. The eRecruit/DOORS Data Administrator identified that [REDACTED] were required for business reasons; however, [REDACTED]

Finally, inspected documented Plans of Actions and Milestones (POA&Ms) and determined that the above deficiencies were not previously identified by management.

CAUSE:

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 7, [REDACTED] dated August 2011, page 3, states that:

The DOL Computer Security Handbook, Edition 4.0, Volume 12, [REDACTED] states that:

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3,

states that:

NIST SP 800-53, Rev.3, Control Area further requires that:

EFFECT:

The use of

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

[Redacted Management Response]

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)

System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)

Finding Number: OASAM-ERD-07-PS.06

Date Provided to Management: September 15, 2012

Date Response Due: September 21, 2012

Title: Deficiency around New Users Rules of Behavior Acknowledgment

CONDITION:

During our FY 2012 audit, we inspected evidence of completion of Rules of Behaviors and determined that 3 of 15 selected new users did not have evidence of acknowledging the Rules of Behavior prior to gaining access to the information system.

Finally, inspected documented Plans of Actions and Milestones (POA&Ms) and determined that the above deficiency was not previously identified by management.

CAUSE:

We were informed by the eRecruit/DOORS Project Manager and the System Administrator and were informed that an automated account management process was not in place to track completion of DOL requirements, New Users, User Recertification, or User Terminations and requests were being tracked manually. A ticketing system which would have improved this process, and others, was previously planned for but had not been implemented due to changing priorities within OASAM.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 1, Version 1.0, dated August 2011, states in 3.1.1 Manage Information System Accounts, page 5, that:

- *Rules of Behavior must be read and acknowledged prior to assuming responsibility for the account of new access permissions.*

National Institute of Standards and Technology (NIST) Special Publication(SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control PS-6, Access Agreements, that:

The organization:

- a. *Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access*

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

EFFECT:

Without proper acknowledgement of the system Rules of Behavior, users have not accepted accountability for their actions, and may be more likely to engage in behavior that could potentially compromise the confidentiality, availability, and integrity of the e-Recruit/DOORS system and job applicant data.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM management concurs with the NOF. Due to inadequate records retention, the three (3) records could not be found for use as evidence during the FY2012 audit cycle – despite the DOORS team support staff having recalled receiving user acknowledgments, via email.

The DOORS team will take corrective actions in FY2013 by creating and documenting a formal approach for better records retention to track and maintain users' acknowledgment of the Rules of Behavior.

OASAM continues to conduct research for a solution to automate the DOORS account management processes (e.g., new user requests; user account recertification; user termination requests; etc.) and ensure efficient and effective account management actions in accordance with DOL policies.

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)

System: e-Recruit/DOL Online Opportunity Recruitment System (DOORS)

Finding Number: OASAM-ERD-08-SA.04

Date Provided to Management: September 15, 2012

Date Response Due: September 21, 2012

Title: Deficiency over Third Party Oversight Policies and Procedures

CONDITION:

During our FY 2012 audit, we inquired with the eRecruit/DOORS Project Manager and System Administrator were informed policies and procedures, including clear responsibilities, had not been established for information security oversight of systems operated on the Organization's behalf. Further, although documents were being obtained from the vendor upon request, we were informed that appropriate evidence for assessing security controls were not defined to ensure security and contractual requirements were being met.

Also, we inspected documented Plans of Actions and Milestones and determined that the above deficiencies were not previously identified by management. Finally, we were informed that no compensating controls were in place.

CAUSE:

The eRecruit/DOORS Project Manager and the System Administrator informed us that oversight responsibilities and expectations are not clearly defined at the Department level. In consequence, the process for contractor oversight was not defined in procedures and obtaining sufficient assurance that security controls and services are effectively implemented and comply with Federal guidelines and DOL policies did not occur.

CRITERIA:

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control SA-04, Acquisitions, that:

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

a. Security functional requirements/specifications;

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

- b. Security-related documentation requirements; and*
- c. Developmental and evaluation-related assurance requirements.*

The DOL Computer Security Handbook, Edition 4.0, Volume 0, Version 1.0, dated October 2011, states in 1.3 Scope and Applicability, page 1, that:

The provisions of these policies pertain to all DOL agencies and information systems. Agency senior management shall ensure that information systems operated by or on behalf of the Department receive adequate security equivalent to the safeguards required of systems operated internally to the Department.

EFFECT:

Without clearly documented information security responsibilities and proper oversight, the agency may not be able to hold the supporting organization accountable should a security breach occur that impacts eRecruit/DOORs processing and applicant data.

Further, not having an understanding of specific responsibilities over each control can lead to the agency assuming the other party is performing a control objective and overlook mitigating the security risks.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM management partially concurs with the Condition, Cause, and Effect. A detail review of the DOORS vendor contract, to ensure all procurement requirements for a third party vendor, is not performed by the DOORS Project Manager and team. Rather, the vendor contract review is the responsibility of the OASAM Procurement staff. In addition, the contract is reviewed to ensure the inclusion of security language, as required by FISMA and DOL. At the time of the original contract, the security related language was sufficient to provide the security expectations and deliverables as described below however, may not be to the detailed level that is expected in a contract for today.

The DOORS Project Manager and team meet with the vendor on a weekly basis (via conference call) and discuss various project initiatives; issues and/or concerns; and possible system resolutions. DOORS security-related agenda items are also added as topics for discussion.

During the audit, the vendor supplies a large volume of NIST-based security related documents that were uploaded into CSAM and made available to the auditors. The material is provided on an annual basis with some of the material updated more frequently.

The vendor employs a third party independent contractor to perform a tri-annual independent assessment of the system, which helps form the basis of the annual self-assessments maintained within CSAM. All CSAM entered data was available, without restriction, to the audit staff that shows the vendor's proactive support for the security requirements defined by DOL and NIST.

Based on the data presented, current deliverables, and coordination efforts, between the vendor and the DOORS Project Management and team, and without further supporting federal requirements dictating specific processes and procedures, OASAM management considers the current processes, procedures, and tools in place sufficient for vendor oversight as currently contracted.

ALVIN BLACK

Agency Representative

Alvin Black

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)
System: e-Recruit/DOL Online Opportunity Recruitment System (e-Recruit/DOORS)
Finding Number: OASAM-ERD-09-[REDACTED]
Date Provided to Management: September 15, 2012
Date Response Due: September 21, 2012
Title: [REDACTED]

CONDITION:

During the FY2012 [REDACTED] assessments, conducted on July 5, 2012, we observed [REDACTED] and determined that [REDACTED] was being performed on eRecruit/DOORS.

We reviewed the [REDACTED] and determined that the following was not tested:

[REDACTED]

Due to this, we could not determine if the implemented controls in place for detecting and preventing [REDACTED] within the eRecruit/DOORS were properly designed and implemented.

Further, despite the [REDACTED] we determined the following on the eRecruit/DOORS Information System;

[REDACTED]

Finally, inspected documented Plans of Actions and Milestones (POA&Ms) and determined that the above deficiencies were not previously identified by management.

**Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012**

CAUSE:

The eRecruit/DOORs Project Manager, System Administrator, and OASAM Security indicated that due to the language in the contract OASAM did not have the appropriate rights to [REDACTED] of the information system.

Further, the third party stated that the [REDACTED] were sufficient to identify any weaknesses and vulnerabilities.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 17, Version 1.0, dated August 2011, states in [REDACTED] that:

[REDACTED]

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in [REDACTED] states that:

[REDACTED]

The DOL Computer Security Handbook, Edition 4.0, Volume 5, Version 1.0, dated August 2011, states in [REDACTED] requirement is:

- [REDACTED]

EFFECT:

[REDACTED]

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

information system. Further, by not adhering to the current security baselines in place, the risk is increased that the system could be exposed to malicious technical attacks or unauthorized/ unintentional changes.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

ALVIN BLACK

Agency Representative

[Signature]

Signature

9-26-12

Date

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

Office: Office of the Assistant Secretary for Administration and Management (OASAM)

System: e-Recruit/DOL Online Opportunity Recruitment System (e-Recruit/DOORS)

Finding Number: OASAM-ERD-10-RA.03

Date Provided to Management: September 21, 2012

Date Response Due: September 28, 2012

Title: Deficiency in Risk Assessment Updates

CONDITION:

We inspected evidence of the risk assessments updated and determined that the following was not evidenced since February 2011, as required by DOL policy:

- Annual review of the Risk Assessment performed by the system owner and Information System Officer (ISO)
- Annual reporting of the Risk Assessment to the appropriate Designated Authorizing Authority (DAA)

CAUSE:

We were informed by OASAM's Information System Officer that Risk Assessments are only vetted and approved by the ISO and the DAA as part of the system's authorization to operate package. The ISO and the DAA were in the review process for a new authorization to operate package, including the risk assessment documents.

CRITERIA:

The DOL Computer Security Handbook, Edition 4.0, Volume 14, Risk Assessment Procedures, dated August 1, 2011, page 7-11 states that DOL Agencies must:

- b. Document risk assessment results in Cyber Security Assessment and Management (CSAM) Tool*
- c. Review risk assessment results at least annually*
- d. Update the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system*
 - *All system changes must be reviewed to determine if they meet the criteria of being a significant change.*
 - *Once an update is performed, the system owner and ISO review the information in CSAM, document the activities as part of the continuous monitoring program, and post the most current risk reports to the CSAM appendices page.*

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

- *The annual review is to be performed by the system owner and ISO and reported to the DAA. The ISO must notify Office of the Chief Information Officer (OCIO) Security via email when the annual review of the risk assessment has been completed and the reports updated in CSAM.*

National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009, states in Control RA-3, Risk Assessments, states that:

The organization:

- c. Reviews risk assessment results [Assignment: organization-defined frequency]; and*
- d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.*

EFFECT:

In today's dynamic environment, without a detailed, qualitative risk assessment, the full extent of threats, risks, and vulnerabilities to information systems may not be understood and adequately considered. Also, appropriate decisions and adjustments to the security policies and procedures may not be made regarding which risks to accept, and which to mitigate through security controls.

Department of Labor (DOL)
Federal Information Systems Management Act (FISMA) - Notification of Findings (NOF)
FY 2012

MANAGEMENT RESPONSE:

OASAM management concurs with the NOF.

The DOORS team will take corrective actions in FY2013, by creating and documenting a Plan of Action and Milestones (POA&M) to ensure the OASAM ISO and DAA obtain and review the Risk Assessment in accordance with DOL Computer Security Handbook.

ALVIN BLACK

Agency Representative

[Signature]

Signature


9-26-12

Date



SEP 26 2012

MEMORANDUM FOR: T. MICHAEL KERR
Chief Information Officer

FROM: 
ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: Alert Memorandum: OALJ is using unauthorized
Apple iPads that are not FIPS 140-2 compliant.
Report Number: 23-12-010-07-001

While auditing the Office of Administrative Law Judges' (OALJ) General Support System, we found that it was using four Wi-Fi 64GB Apple iPads purchased on September 30, 2011, for \$2,761, and three Wi-Fi + 3G Verizon 32GB Apple iPads purchased on November 21, 2011, for \$1,947. OALJ stated that they were using the iPads to access email and review attachments dealing with legal casework, including taking notes and scheduling meetings.

According to the Department of Labor (DOL) Computer Security Handbook (CSH), "Wireless technologies/devices used for storing, processing, and/or transmitting information must first be approved by the Office of the Chief Information Officer, through the EA¹ governance process prior to implementation." OALJ did not acquire this approval.

The iPads do not meet the encryption requirements of Federal Information Processing Standard (FIPS) 140-2. According to Department of Labor Manual Series 9, Chapter 1200, "Use of any portable device or media without encryption must be approved in writing by the Deputy Secretary of Labor or his/her designee. In accordance with the process outlined in the DOL Computer Security Handbook, data on the portable device or media must be determined, in writing, to be non-sensitive before approval will be granted by the Deputy Secretary or his/her designee. Agencies seeking an exemption to the encryption requirement must use the approval form as well as follow the process contained in the DOL Computer Security Handbook." This policy is expanded further by the DOL CSH Access Control procedures which require that "Use of any portable and mobile

¹DLMS 9 Chapter 500 states "Enterprise Architecture (EA) is defined within the Clinger-Cohen Act of 1996 as Information Technology Architecture (ITA) and further as "an integrated framework for evolving or maintaining existing IT, and acquiring new IT to achieve the agency's strategic goals and information resources management goals" (Section 5125 (d))."

device that does not employ FIPS 140-2 compliant encryption must be approved in writing by the Deputy Secretary.” OALJ did not obtain this approval prior to using the iPads. The agency provided in response to OIG’s Notice of Finding screen shots of the iPads’ settings to demonstrate the agency enabled the Apple encryption; however, approval for its use is still required.

The use of unauthorized wireless devices that do not employ FIPS 140-2 compliant encryption could compromise sensitive data or personally identifiable information. Therefore, we recommend the Chief Information Officer:

1. Assist the Deputy Secretary in determining whether the use of the iPads is appropriate and the security requirements meet current Federal information system security standards or compensating controls are adequate.
2. Increase agency awareness of the requirements for obtaining and using emerging technologies.

Please respond to this report within three business days with a corrective action plan. If you have any questions, please contact Keith Galayda, Audit Director, at (202) 693-5259.

cc: Edward Hugler
Tonya Manning
Stephen L. Purcell
Victor V. Soto
P.J. Soto

U.S. Department of Labor

Office of Inspector General—Office of Audit

OFFICE OF THE CHIEF INFORMATION OFFICER



THE DEPARTMENT OF LABOR NEEDS A BETTER PROCESS TO SANITIZE ELECTRONIC MEDIA PRIOR TO DISPOSAL

NOTICE:

**THIS REPORT CONTAINS SENSITIVE INFORMATION AND IS
RESTRICTED TO OFFICIAL USE**

This report is being provided to agency officials solely for their review, comment, and appropriate action. It contains sensitive information, which should only be reviewed by individuals with a legitimate "need to know." Recipients of this report are not authorized to distribute or release it without the express permission of the Office of the Inspector General.

A handwritten signature in purple ink that reads "Elliott P. Lewis".

Assistant Inspector General for Audit
U.S. Department of Labor

Date Issued: March 29, 2013
Report Number: 23-13-006-07-001

BRIEFLY...

Highlights of Report Number 23-13-006-07-001, "The Department of Labor Needs A Better Process to Sanitize Electronic Media Prior to Disposal," issued to the Chief Information Officer.

WHY READ THE REPORT

Federal regulations mandate that government agencies protect data about individuals from unauthorized release and establish policies and procedures to protect licensed software and sensitive data stored on electronic media before its release, transfer, or disposal.

WHY OIG CONDUCTED THE AUDIT

In 2003, we found unsanitized computers that had been designated for disposal. In a 2005 follow-up audit, we found unsanitized computer hard drives that contained licensed operating system software, licensed application software, and unencrypted data of a sensitive, personal, or confidential nature that had been designated for disposal. Given these previous findings, we conducted an audit to answer the following question:

Did DOL effectively sanitize electronic media prior to its transfer or disposal?

READ THE FULL REPORT

This report contains sensitive information and is restricted to official use only. As such, this report is only available by written request to the OIG Disclosure Officer. For instructions on making the request, go to: <http://www.oig.dol.gov/foia.htm>.

March 2013

THE DEPARTMENT OF LABOR NEEDS A BETTER PROCESS TO SANITIZE ELECTRONIC MEDIA PRIOR TO DISPOSAL

WHAT OIG FOUND

DOL did not always effectively sanitize electronic media prior to its transfer or disposal. At [REDACTED], we found unsanitized hard drives that contained DOL information and personal documents, equipment discarded in a trash receptacle, and inventoried equipment designated for disposal that could not be physically located. At the Bureau of Labor Statistics' (BLS)(b) (7)(E) office, we found unsanitized media that contained sensitive information, as well as an inventory listing of hard drives that could not be physically located.

Our testing [REDACTED] regional offices operated by OASAM did not identify any issues or weaknesses.

WHAT OIG RECOMMENDED

We recommend the CIO implement effective electronic media sanitization practices for preventing the unintentional release of DOL information and establish effective monitoring of DOL agencies' media sanitization procedures.

The OASAM Deputy Assistant Secretary for Operations (DASO) responded for the CIO stating that OASAM management is fully prepared to implement the appropriate corrective actions to address the report's recommendations. Also cited was improving the controls and practices that ensure 100 percent destruction of electronic media capable of holding information through vendor contracted services and performing quarterly random sampling verification.

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Assistant Inspector General’s Report	1
Results In Brief	2
Objective — Did DOL effectively sanitize electronic media prior to its transfer or disposal?	3
<i>Without improvements to media sanitization controls and practices, unintentional release of sensitive information may occur.</i>	<i>3</i>
National Office Hard Drives Not Sanitized	3
BLS Hard Drives Not Sanitized.....	3
Recommendations	5
Appendices	
Appendix A Objective, Scope, Methodology, and Criteria	9
Appendix B Abbreviations	11
Appendix C OASAM's Response to the Draft Report	13

PAGE INTENTIONALLY LEFT BLANK

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210



March 29, 2013

Assistant Inspector General's Report

T. Michael Kerr
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave. NW
Washington, DC 20210

Federal regulations mandate that government agencies protect data about individual citizens from unauthorized release and establish policies and procedures to protect licensed software and sensitive data stored on electronic media before its release, transfer, or disposal. The Chief Information Officer (CIO) is responsible for implementing controls and practices, including properly sanitizing electronic media to protect the Department of Labor's (DOL) information. In 2003, the Office of Inspector General (OIG) tested 21 computers identified as sanitized and ready for disposal and found licensed software or recoverable data.¹ In a 2005 follow-up audit, we found national office computer hard drives identified as sanitized and ready for transfer or disposal that contained licensed operating system software, licensed application software, and unencrypted data of a sensitive, personal, or confidential nature.² Given these previous findings, we conducted an audit to answer the following question:

Did DOL effectively sanitize electronic media prior to its transfer or disposal?

We tested DOL's applicable policies, procedures, and practices to ensure internal controls were working as intended and electronic media were properly sanitized for the period January 6, 2012, through August 12, 2012. We performed audit work in

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

¹ Alert Report Number 23-03-009-04-001, "Electronic Media Disposal," dated March 27, 2003.

² Audit Report Number 23-05-028-50-598, "DOL Needs to Perform Electronic Media Sanitization More Effectively Prior to Transfer or Disposal," dated September 30, 2005.

Results In Brief

DOL did not always effectively sanitize electronic media prior to its transfer or disposal. At DOL's national office, we found unsanitized hard drives that contained DOL information and personal documents, and equipment discarded in a trash receptacle. We also noted that inventoried equipment designated for disposal could not be physically located. At the Bureau of Labor Statistics (b) (7)(E) office, which the Office of the Assistant Secretary for Administration and Management (OASAM) had authorized to directly dispose its equipment following its own policies and procedures, we found unsanitized media that contained sensitive information, as well as an inventory listing of hard drives that could not be physically located. However, our testing in three regional offices operated by OASAM did not identify any issues or weaknesses.

OIG's Conclusion and Recommendations

Controls and practices intended to mitigate previously identified weaknesses were not working as intended. To prevent further unintentional release of DOL information, we recommend the CIO implement effective electronic media sanitization practices for preventing the unintentional release of DOL information and establish effective monitoring of DOL agencies' media sanitization procedures.

OASAM's Response

OASAM's Deputy Assistant Secretary for Operations (DASO) responded for the CIO stating that OASAM management is fully prepared to implement the appropriate corrective actions to address our report's recommendations. The DASO also said the CIO would improve controls and practices to ensure 100 percent destruction of electronic media capable of holding information by contracting with a vendor and performing quarterly random sampling verification with the vendor to ensure the disposed media has been sanitized. OASAM's response is included in its entirety in Appendix C.

The OIG examined the full response and determined the planned corrective actions align with the OIG's recommendations.

RESULTS AND FINDINGS

Objective — Did DOL effectively sanitize electronic media prior to its transfer or disposal?

Without improvements to media sanitization controls and practices, unintentional release of sensitive information may occur.

National Office Hard Drives Not Sanitized

DOL did not always effectively sanitize electronic media prior to its transfer or disposal. From our testing of the 55 hard drives identified for disposal in the [REDACTED] we found 4 contained government and personal information. For example, on 1 hard drive we found an employee's Standard Form 50, birth certificate, and personal resume. These documents contained the employee's name, social security number (SSN), date of birth, and position title.

In addition, we found two desktop computers in a trash receptacle on the [REDACTED]. While the computers contained no hard drives, the hard drives that had been used in the computers were unaccounted for in the agency's records.

BLS Hard Drives Not Sanitized

From our testing of the 60 hard drives identified for disposal in the [REDACTED], we found 3 had not been sanitized and contained sensitive information and personally identifiable information. We also found 1 computer and 2 hard drives missing from the BLS disposal manifest. BLS could not tell us where the missing equipment was located.

The first unsanitized hard drive belonged to a [REDACTED] (b) (7)(C). This hard drive contained [REDACTED] and data, including raw data files dealing with [REDACTED] (b) (7)(E). In addition, we found hundreds of the user's personal pictures, the user's Form W-2, and the user's Citibank government travel card application that contained name, SSN, date of birth, residential address, email address, and phone number.

The second unsanitized hard drive belonged to a [REDACTED] (b) (7)(C) in the [REDACTED]. This hard drive contained information from foreign dignitaries. For example, we found names, dates of birth, and positions held for officials of the Russian government.

The third unsanitized hard drive belonged to a [REDACTED] (b) (7)(C) in the Division of [REDACTED]. This hard drive contained files with [REDACTED]

the names, dates of birth, and SSNs of 189 current and separated DOL employees. There was also an Equal Employment Opportunity Commission form containing the SSN of the user.

These results demonstrate weaknesses in the procedures and monitoring used to ensure electronic media were properly sanitized prior to disposal.

Media Sanitization Procedures Inadequate

DOL's national office could not ensure 100 percent of its equipment was being sanitized. On one pallet waiting to be transferred, there was sanitization documentation for 26 information technology (IT) items missing documentation, 16 items had incorrect property descriptions on the sanitization listing and 3 computers listed on the documentation were missing from the pallet.

On March 22, 2012, DOL granted BLS authority to directly dispose of its equipment based on procedures that required the BLS Office of Technology and Survey Processing, Division of Network and Information Assurance, to conduct internal audits of its designated disposals. Although the BLS internal auditors did not find any unsanitized equipment, we found 3 unsanitized hard drives during our audit that contained business, sensitive, personal, or confidential information. This occurred for two reasons. First, BLS internal auditors sampled just 10 percent of all disposals for testing. This sampling methodology was not sufficient to provide reasonable assurance the equipment was properly sanitized. Second, BLS internal auditors did not include broken computers in its sample even though the hard drives still contained data.

Insufficient Monitoring of Performance

We determined OASAM did not coordinate with the Office of the Chief Information Officer (OCIO) to ensure DOL agencies documented their measures against unintentional release of information when processing equipment for disposal or donating it outside of DOL as required by Department of Labor Manual Series (DLMS) 9 Information Technology, chapter 300. In addition, the OCIO did not perform periodic reviews of DOL agencies' equipment accountability and inventory procedures to ensure they met all legal requirements or policies for government information and information technology management, including compliance with appropriate methods of sanitization of IT equipment and electronic media before disposal as required by DLMS 9 Information Technology, chapter 300.

Because our fieldwork during this audit indicated that DOL had not established or implemented policies and procedures to prevent the unintentional release of sensitive data stored on electronic media, we issued Alert Memorandums to the CIO on March 1, 2012, and June 19, 2012, recommending a moratorium on the release of surplus computers until hard drives could be sanitized. We also recommended the CIO update policies and provide guidance to DOL agencies in this area. In response to those Alert Memorandums, the CIO took immediate corrective action, declaring a

moratorium on the release of surplus electronic media and updating disposal procedures to address the sanitization of electronic media.

During the preparation of this report, OASAM informed us that it resumed disposing electronic media at the DOL national office by sanitizing, then destroying, all hard drives and memory contained in the computers. Also, according to the agency, disposal of each computer was documented with a certificate of destruction identifying each item.

Without fully implementing effective practices and monitoring for electronic media sanitization, DOL and its agencies risk the unintentional release of sensitive information.

RECOMMENDATIONS

We recommend the Chief Information Officer:

1. Fully implement effective electronic media sanitization practices for preventing the unintentional release of DOL information.
2. Fully implement effective monitoring practices for testing DOL agencies' sanitization of IT equipment and electronic media before disposal.

We appreciate the cooperation and courtesies that DOL personnel extended to the Office of Inspector General during this audit.



Elliot P. Lewis
Assistant Inspector General for Audit

PAGE INTENTIONALLY LEFT BLANK

Appendices

PAGE INTENTIONALLY LEFT BLANK

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

Objective

Did DOL effectively sanitize electronic media prior to its transfer or disposal?

Scope

Our audit reviewed the sanitization and disposal of electronic media by DOL agencies in place during fiscal year 2012. We judgmentally and non-statistically selected electronic media scheduled for disposal. Equipment for excess included items identified to be discarded, transferred, decommissioned or otherwise disposed, including computers, laptops, hard drives, printers, fax machines and monitors. We then tested the electronic media scheduled for disposal to determine if it was sanitized.

The audit work was done in the following locations: (b) (7)(E)

Methodology

We acquired electronic media scheduled for disposal from various sources and locations in DOL to determine if sanitization had occurred. We also performed work to determine DOL agencies' compliance with federal, DOL, and agency policies and procedures.

We selected electronic media scheduled for disposal from spreadsheets maintained by DOL to track disposals. From the 142 pieces of IT equipment in (b) (7)(E) scheduled for disposal, we randomly chose 55 items for testing. From the 287 pieces of IT equipment in the (b) (7)(E) scheduled for disposal, we randomly chose 60 items for testing. Due to the limited number of items being disposed in the regions, we judgmentally tested all items scheduled for disposal in the regional offices. We tested 43 items in (b) (7)(E).

We used (b) (7)(E) to test the level and effectiveness of the sanitization.

To understand the federal and DOL requirements of the electronic media sanitization and disposal process, we obtained an understanding of the information listed in the criteria section. We reviewed OASAM policies and procedures related to the disposal of surplus electronic media. We also reviewed the policies and procedures of DOL agencies to ensure compliance with DOL policy.

Criteria

We used the following criteria to perform this audit:

- Federal Information Security Management Act of 2002
- DLMS 2 Administration, Chapter 100 – DOL Property Management
- DLMS 9 Information Technology, Chapter 300 – Management and Accountability of Information Resources
- Computer Security Handbook, Version 4 Volume 0 – Information Security Policies
- Computer Security Handbook, Version 4 Volume 10 – Media Protection Procedures
- National Institute of Standards and Technology Special Publication 800-53 (Revision 3) – Recommended Security Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization

Appendix B

Abbreviations

BLS	Bureau of Labor Statistics
CIO	Chief Information Officer
DLMS	Department of Labor Manual Series
DOL	Department of Labor
IT	Information Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
SSN	Social Security Number

PAGE INTENTIONALLY LEFT BLANK

Appendix C

OASAM's Response to the Draft Report

U.S. Department of Labor

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



MAR 27 2013

MEMORANDUM FOR ELLIOT P. LEWIS

Assistant Inspector General for Audit

FROM:

EDWARD C. HUGLER
Deputy Assistant Secretary for
Administration and Management

SUBJECT:

Department of Labor Needs Better Process to Sanitize
Electronic Media Prior To Disposal
Draft Report No. 23-13-006-07-001

This memorandum responds to the above-referenced Fiscal Year 2013 draft audit report issued on March 20, 2013. The stated audit objective was to determine if the Department effectively sanitized electronic media prior to its transfer or disposal. The audit report concluded that controls and practices were not working as intended and provided two recommendations requiring a management response.

Management is fully prepared to implement the appropriate corrective actions to address the recommendations outlined in the report. Management's response follows:

Recommendations

1. Fully implement effective electronic media sanitization practices for preventing the unintentional release of DOL information.

Response: As noted in the draft audit report, OASAM's Business Operations Center has responsibility for overseeing the disposal process for electronic media at the DOL National Office. The purpose of this process is to ensure that sensitive information is not unintentionally released.

To improve the controls and practices that comprise this disposal process for electronic media disposal through the DOL National Office, management has entered into a contract that ensures 100-percent destruction of electronic media capable of holding information. Under the contract the vendor tracks computers or separate hard drives by (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Management considers this recommendation closed pending OIG validation.

2. Fully implement effective monitoring practices for testing DOL agencies' sanitization of IT equipment and electronic media before disposal.

Response: OASAM is confident that the unintended exposure of DOL information on media set for disposal is all but eliminated given the implemented procedures of sanitization and destruction outlined above. On a (b) (7)(E) basis, the OASAM Business Operations Center will

(b) (7)(E)

Management considers this recommendation resolved with closure dependent on the completion of the corrective action mentioned above and OIG validation.

We appreciate the opportunity to provide input and look forward to the continued collaboration with your office. Please have your staff contact Tonya Manning (Manning.Tonya@dol.gov or (202) 693-4431) or Phil Puckett (Puckett.Philip@dol.gov or (202) 693-6650) for additional discussion. If you have questions or would like to discuss further, please contact me directly at (202) 693-4040.

cc: T. Michael Kerr, Chief Information Officer
Dawn Leaf, Deputy Chief Information Officer
Phil Puckett, Director, Office of Administrative Services

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