



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document:	<b>Significant Department of Labor (DOL) Unimplemented Recommendations and the Email Distribution List Report, 2002 - 2008</b>
Requested date:	01-December-2008
Released date:	21-August-2009
Posted date:	28-October-2009
Source of document:	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 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.



AUG 21 2009

This is in response to your December 1, 2008, Freedom of Information Act (FOIA) request (29017) for the Significant DOL Unimplemented Recommendations and the Email Distribution List Report.

Enclosed are all documents responsive to this request. However, portions of pages containing the names of, and details concerning, specific information systems, recommendations, as well as the identity of an individual involved in the reporting of a computer security incident have been deleted.

These portions, if released, could allow individuals with reasonable information technology skills to gain unauthorized access to agency systems that contain personal or financial information. This information has been redacted pursuant to 5 U.S.C. 552 (b)(2), "high" b2, which protects from disclosure, internal agency information, the release of which, exposes the agency information systems to risk of circumvention or harm by gaining access with intent to manipulate or steal, personal or financial information, and avoid detection.

In addition, the identity of an individual involved in a computer security incident has been withheld pursuant to 5 U.S.C. 552(b)(6) and (b)(7)(C). Exemption 6 authorizes the withholding of names and details of personal information contained in personal, medical, and similar files, which if disclosed to the public, would constitute an unwarranted invasion of personal privacy. Exemption (b)(7)(C) of the FOIA authorizes the withholding of names and details of personal information related to various individuals that are contained in investigative files which, if disclosed to the public, could reasonably be expected to constitute an unwarranted invasion of personal privacy.

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.29017, 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.

Fees were waived for this request.

Sincerely,

Kimberly Pacheco  
Disclosure Officer

Enclosures  
52 pages

U.S. Department of Labor

Office of Inspector General  
Washington, D.C. 20210



JAN 31 2008

The Honorable Henry A. Waxman  
Chairman  
Committee on Oversight and Government Reform  
United States House of Representatives  
Washington, DC 20515-6143

Dear Mr. Chairman:

In response to your request dated December 7, 2007, I am enclosing our report on recommendations my office has made to the Department of Labor between January 1, 2001, and December 31, 2007, that have not been implemented by the Department or by Congress.

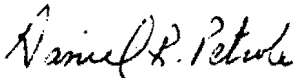
Based on a discussion between Alison Cassady of your office and Susan Carnohan and Jeanine Wagner of my staff on December 18, 2007, we focused on those recommendations made during the period that we considered particularly significant to the Department's mission. Generally, the Enclosure describes significant recommendations that are programmatic in nature or that address controls that are critical to the protection of information technology assets, including personally identifiable information.

We did not include recommendations addressed to specific non-Federal entities, such as grantees and contractors, with two exceptions. First, we included recommendations on hurricane-related benefits paid by the Unemployment Insurance and Disaster Unemployment Assistance programs, which the Department of Labor administers in partnership with the various States. Second, we included recommendations arising from our audits of the Job Corps program, which the Department of Labor operates through direct contracts to private entities or, in some cases, through Memoranda of Understanding with the Departments of Agriculture and Interior. We did not include recommendations from audits of Department of Labor grantees pursuant to the Single Audit Act. These audits are not conducted by the Office of Inspector General, but rather by independent public accountants through contracts or other arrangements with the grantees. The Office of Inspector General's role with respect to such audits is limited to assuring that they meet Government Auditing Standards and that the recommendations are provided to the Department for appropriate action.

The recommendations highlighted in the Enclosure represent a range of the Department's diverse and important mission, from assuring the safety and health of our Nation's miners to protecting retirement benefits. We believe that full implementation of these recommendations could improve the delivery of benefits and services and produce considerable savings for the Department.

Please contact me at 202-693-5100 if you have any questions or would like a briefing on this. Alternatively, your staff may contact Susan Carnohan with any questions or concerns.

Sincerely,



Gordon S. Heddel  
Inspector General

Enclosure

**TABLE OF CONTENTS**

- 1. Coal Mine Safety and Health: Strengthen the Coal Mine Hazardous Condition Complaint Process**
- 2. Coal Mine Safety and Health: Strengthen the Office of Coal Mine Safety and Health's Accountability Program**
- 3. Mine Safety and Health: Improve Controls Over Performance Data**
- 4. Employee Pension Plans: Improve Oversight of Cash Balance Lump Sum Distributions**
- 5. Employee Benefit Plan Audits: EBSA Needs Additional Authority to Improve the Quality of Employee Benefit Plan Audits**
- 6. Employee Benefit Plan Annual Reports: Mandate Electronic Filing of Annual Reports by Employee Benefit Plans**
- 7. Unemployment Insurance: Work Toward Legislative Change to Require Employers to Report a New Hire's First Day of Earnings**
- 8. Unemployment Insurance: Analyze and Address the Causes of Unemployment Insurance Overpayments Identified Through the Benefit Accuracy Measurement Program**
- 9. Hurricanes Katrina and Rita: Tighten Controls Over Disaster-related Unemployment Benefits**
- 10. Employment Discrimination Against Veterans: Conduct More Timely Investigations of Veterans' Employment Discrimination Complaints**
- 11. Workforce Investment Act: Seek Support for Changes to Workforce Investment Act Training Provisions**
- 12. Discretionary Grants: Document All Decisions and Discussions That Lead to Actions by DOL Officials That Affect How and to Whom Grant Funds Are Distributed**
- 13. Job Corps: Strengthen Efforts to Identify Students with Unknown or Undisclosed Cognitive Disabilities**

14. **Job Corps Performance Data: Improve Monitoring of Job Corps Performance Data**
15. **Procurement (cross-cutting recommendations): Create Organizational Separation Between DOL Procurement and Program Functions**
16. **Information System Security: Remedy Information Security Control Weaknesses That Could Compromise Information or Result in Disruptions in the Delivery of Program Services**
17. **Unemployment Insurance Disaster Recovery Plans: Ensure that Contingency Planning Weaknesses in State Workforce Agencies' Unemployment Systems Are Corrected to Prevent the Disruption of Benefits to Unemployed Americans**
18. **Protection of Personal Identifiable Information: Implement Information Security Controls to Reduce the Risk of Exposing Personally Identifiable Information to Unauthorized Access and Use**

# Coal Mine Safety and Health

---

## 1. Strengthen the Coal Mine Hazardous Condition Complaint Process

**Summary of Audit:** We conducted a performance audit of the hazardous condition complaint process managed by the Mine Safety and Health Administration's (MSHA) Office of Coal Mine Safety and Health (CMS&H). While MSHA operates hazardous condition complaint processes for both coal mines and metal/nonmetal mines, this audit focused only on the process related to coal mines. The hazardous condition complaint process is the mechanism in place to satisfy statutory requirements for immediate mine inspections in response to certain alleged hazards. It is critically important that the process work effectively to give miners and their representatives a voice and a means to ensure appropriate and prompt action is taken to remove hazardous conditions from the nation's coal mines. Additionally, the recent increase in coal mine fatalities underscores the need to continuously improve processes that minimize safety and health risks in the coal mines.

**Findings:** We found that CMS&H had made efforts to improve the hazardous condition complaint process. For example, CMS&H had significantly expanded the Mine Act's definition of a "complaint" that required its action. In addition, CMS&H also investigated verbal complaints, unsigned or anonymous complaints, and complaints originating from someone other than the miner or miner's representative. We also found that development of an overall strategy for promoting the hazardous condition complaint process would help ensure promotional efforts by CMS&H's 11 districts are consistent and complete. Additionally, CMS&H had not ensured effective performance by the contractor used to receive complaints filed with MSHA headquarters. A significant number of hazardous condition complaints filed with MSHA headquarters and directly with the districts were not evaluated or inspected timely. These delays may have subjected miners to prolonged hazardous conditions. Further, process improvements are needed to ensure complaint evaluations and inspections are thorough, consistent, and in accordance with the Mine Act and MSHA policy. CMS&H management analysis relied on reports that were based on complaints filed solely with MSHA headquarters; about one-third of the total complaints. The reports did not include complaints filed directly with the districts. Additionally, information reported to the public on hazardous condition complaints was incomplete.

**Recommendations:** We made 13 recommendations, summarized as follows: ensure efforts to promote the hazardous condition complaint process are planned, monitored and evaluated, and complaints are recorded accurately and completely; ensure the expectation of evaluation and inspection timeliness is quantified and that timeliness is monitored and systemic reasons for delays are identified and addressed; ensure complaint evaluations and inspections are consistent and in accordance with the Mine Act and MSHA policy; and ensure complaint information used by CMS&H to manage the process or reported to the public is complete.

# Coal Mine Safety and Health

---

## 1. Strengthen the Coal Mine Hazardous Condition Complaint Process

**Status:** MSHA initiated or planned corrective action to address 12 of our 13 recommendations. MSHA did not agree to quantify the expectation of timeliness in specific terms for beginning inspections of "imminent danger" allegations. MSHA believed that the time requirements stated in the Mine Act and Federal regulations ("immediately" and "as soon as possible") adequately established the expectation for inspection timeliness. MSHA stated that a performance metric for inspection timeliness was too binding, and may force abandonment of the current approach on accepting hazardous condition complaints beyond the 103(g) complaints filed in writing by miners and miner representatives.

**Report:** 05-06-006-06-001, Issued September 29, 2006



# Coal Mine Safety and Health

---

## **2. Strengthen the Office of Coal Mine Safety and Health's Accountability Program**

**Summary of Audit:** Based on our ongoing assessment of MSHA's safety and health programs and responsibilities, we initiated an audit of MSHA's Accountability Program within its Office of Coal Mine Safety and Health (CMS&H). We focused on the Accountability Program within CMS&H in part because of the increase in coal mining accidents during CY 2006. As of December 31, 2006, there had been 47 fatalities in the coal mining sector, as opposed to 28 and 22 coal mining fatalities reported for CYs 2004 and 2005, respectively. The Accountability Program was established to evaluate the quality of MSHA enforcement activities by conducting peer reviews of District activities, and to provide reasonable assurance that policies and procedures are being complied with consistently throughout Coal Mine Safety and Health.

**Findings:** We found that MSHA's Accountability Program, as designed, did not provide adequate assurance that CMS&H's oversight responsibilities were effectively and consistently performed. Specifically, the selection of which enforcement activities to review did not rely primarily on measures of internal performance and was usually restricted to only a portion of CMS&H's area of responsibility. Also, the selection of which enforcement activities to review could be influenced to prevent negative results. We also found that accountability reviews did not always: (1) include mine visits, (2) assure the independence of review teams, (3) include a consistent type or depth of analyses, or (4) include interviews of appropriate individuals. As a result, CMS&H officials lacked assurance that the Accountability Program was adequately and consistently implemented nationwide. Finally, we found that CMS&H did not effectively use the results of its accountability reviews to improve its operations timely and consistently.

**Recommendations:** We made 14 recommendations, summarized as follows: ensure that the selection of enforcement activities for review during HQRs and DPRs rely primarily on measures of internal performance; ensure the election of which enforcement activities to review during DPRs cannot be influenced to prevent negative results; include mine visits during DPRs; ensure the independence of DPR review teams; ensure a consistent type or depth of analyses during DPRs; use a standard format for DPR reports; ensure the timely development, implementation, and monitoring of corrective actions; use a centralized tracking system; and ensure that identified common deficiencies, corrective actions, and best practices are communicated.

**Status:** MSHA has established an Office of Accountability to ensure that management controls, including controls over Accountability Reviews, are in place and fully implemented. MSHA is also revising the MSHA Accountability Program and Accountability Program Handbook to reflect many of the

## Coal Mine Safety and Health

---

### **2. Strengthen the Office of Coal Mine Safety and Health's Accountability Program**

recommendations made in our report, and states that the new Handbook will be issued in April 2008.

**Report: 05-07-002-06-001, issued September 29, 2007**

# Mine Safety and Health

---

## 3. Improve Controls Over Performance Data

**Summary of Audit:** We conducted a performance audit to determine the completeness and reliability of the CY 2003 data used to support the Mine Safety and Health Administration's (MSHA) FY 2003 performance goals related to the agency's efforts to reduce (1) mine injuries and fatalities, and (2) miners' exposure to health hazards such as coal and silica dust and excessive noise levels. MSHA's FY 2003 performance goals called for the agency to reduce the mine industry fatal injury occurrence rate by 15 percent annually and reduce the all injury occurrence below the FY 2000 baseline by the end of FY 2005.

**Findings:** We could not determine reliability of MSHA's reported all-injury occurrence rate. The all-injury occurrence rate is measured as injuries and fatalities per 200,000 hours worked. MSHA could not ensure it had accounted for all hours worked because it did not require mine operators to submit documentation that supports the amount of contractor hours worked. In addition, our audit found that MSHA did not have complete and reliable data to support the testing conducted to ensure noise exposure levels did not exceed established limits.

**Recommendations:** We recommended that mine operators report all hours worked for both employees and contractors to allow verification that all data needed to support the reported injuries and fatalities have been included; mine operators submit or maintain, and mine inspectors review as part of their normal inspection process, documentation that supports the amount of hours worked by mine employees and contractors; controls be developed and put in place to adhere to procedures that require systematic and regular entry of noise sample data into MSHA's tracking systems.

**Status:** MSHA disagreed with our recommendations related to the need to capture and report hours worked by contractors. On September 4, 2007 OMB issued Bulletin 07-04, "Audit Requirements for Federal Financial Statements." The Bulletin states that, starting in fiscal year 2008, auditors are not required to test internal controls related to performance information. MSHA states that the Bulletin clarifies audit requirements for performance information in a manner that supports MSHA's position. We disagree. MSHA remains responsible for ensuring the validity of its performance information, regardless of whether or not an audit of this information is mandatory.

MSHA stated that it has developed appropriate controls for entry of noise sampling data into the Coal Mining Safety and Health Information System. Corrective action related to MSHA's Metal Nonmetal Management Information System has not been finalized.

**Report:** 22-07-008-06-001, Issued September 29, 2006

# Employee Pension Plans

---

## 4. Improve Oversight of Cash Balance Plan Lump Sum Distributions

**Summary of Audit:** We conducted a performance audit to determine if the Employee Benefits Security Administration (EBSA), formerly the Pension Welfare Benefits Administration, was adequately protecting participants' benefits when defined benefit pension plans were converted to cash balance plans. Private pension plans are governed primarily by two laws: The Employee Retirement Income Security Act of 1974 as amended (ERISA), and the Internal Revenue Code (IRC). EBSA enforces ERISA's reporting and disclosure provisions and fiduciary standards that cover how plans should operate in the best interest of participants. The Internal Revenue Service (IRS) enforces participation, vesting, and funding standards for pension plans. When we conducted our audit in 2002, industry estimates stated that since the mid-1980s between 300 and 700 traditional defined benefit pension plans had converted to cash balance plans. One estimate indicated these conversions affected over 8 million working Americans and involved pension assets of over \$334 billion. EBSA had devoted considerable resources on cash balance plans, focusing on disclosure and education, but had not devoted significant enforcement resources to protecting participants' benefits.

**Findings:** Our audit of 60 converted cash balance plans found that the conversions adequately protected benefits from earlier plans. However, in 13 of those 60 plans, workers who left employment before normal retirement age did not receive all the accrued benefits to which they were entitled, and had been underpaid an estimated \$17 million each year. Applying the same estimation model used in our judgmental sample to the estimated 300 to 700 defined benefit plans that had converted to cash balance plans, we estimated that workers may have been underpaid between \$85 million and \$199 million annually.

**Recommendations:** We recommended that EBSA direct more enforcement resources to protecting cash balance plans' participant benefits, initiate specific enforcement action on the 13 plans with forfeitures identified in our audit, and work with IRS to develop improved guidance for plan administrators in calculating participant accrued benefits.

**Status:** EBSA disagreed with our conclusions and stated that, without a broader survey of the problem and more detailed information, it could not commit to redirecting enforcement resources to cash balance plan benefit calculations. EBSA referred the 13 plans with participant underpayments to the IRS for technical review of each plan's benefit formula. According to EBSA officials, IRS has not yet initiated its review of the referred cases but has informed EBSA that it intends to do so by the end of 2008. Action on improving guidance for plan administrators has been delayed, pending the outcome of IRS' review of the 13 referred plans.

**Report:** 09-02-001-12-121, issued March 29, 2002

## Employee Benefit Plan Audits

---

### **5. EBSA Needs Additional Authority to Improve the Quality of Employee Benefit Plan Audits**

**Summary of Audit:** We conducted a performance audit to evaluate the effectiveness of the Employee Benefits Security Administration's (EBSA) process to identify and correct substandard employee benefit plan audits. The Employee Retirement Income Security Act (ERISA) requires that most large employee benefit plans obtain an annual audit of their financial statements. In Fiscal Year 2001, retirement plan administrators filed about 65,000 financial statements on private pension plans holding assets over \$4 trillion and covering over 88 million participants. EBSA is responsible for ensuring that employee benefit plan audits meet ERISA requirements, including professional standards, to help protect participant and beneficiary benefits. Prior reviews had shown that a significant number of these audits did not meet ERISA requirements. These substandard audits did not provide participants and beneficiaries the protections envisioned by the Congress. To deal with this problem, EBSA established an Office of Chief Accountant (OCA). One of OCA's main responsibilities is to ensure the quality of employee benefit plan audits. As part of an overall enforcement and compliance assistance effort, OCA implemented a program in 1990 to identify and correct substandard audits.

**Findings:** We found that, although EBSA had reviewed a significant number of employee benefit plan audits and had made efforts to correct substandard audits, including rejecting annual report filings and making referrals to professional organizations, the process for identifying and correcting substandard employee benefit plan audits was not effective. EBSA did not have sufficient enforcement authority to ensure that employee benefit plan audits adequately protected participants. Although EBSA has the responsibility to enforce ERISA's audit requirements, ERISA did not grant EBSA enforcement powers over the auditors performing employee benefit plan audits. In fact, EBSA had much less enforcement capabilities than other Federal agencies with similar responsibilities, such as the Securities and Exchange Commission and Internal Revenue Service. As a result, EBSA could not take direct enforcement action against the plan auditor for substandard audit work. EBSA could only take indirect enforcement action by imposing civil penalties against the plan administrator, the person who engages a plan auditor.

**Recommendation:** We recommended that the Assistant Secretary for Employee Benefits Security propose changes to ERISA to grant EBSA greater enforcement authority over such matters as registration, suspension, debarment, and civil penalties against employee benefit plan auditors.

**Status:** The Department has unsuccessfully sought legislative changes to obtain more authority over plan auditors and the scope of plan audits.

**Report:** 09-04-005-12-121, issued September 30, 2004

# Employee Benefit Plan Annual Reports

---

## 6. Mandate Electronic Filing of Annual Reports by Employee Benefit Plans

**Summary of Audit:** We conducted a performance audit of the Employee Benefits Security Administration's (EBSA) ERISA Filing and Acceptance System (EFAST) to determine if EFAST accurately captured data submitted on Form 5500 filings submitted by employee benefit plans. The Employee Retirement Income Security Act of 1974 (ERISA) requires employee benefit plans to submit annual reports, and the Form 5500 was developed for this purpose. EFAST is EBSA's system for processing Form 5500s, processing about 1.2 million Form 5500s per year and distributing data to the Internal Revenue Service, Pension Benefit Guaranty Corporation, and EBSA. These agencies use EFAST data to meet their legislatively mandated missions to protect the pensions and other employee benefits of the American workforce. When we conducted our audit in 2005, ninety-nine percent of the Form 5500s were submitted on paper; the remaining 1 percent were electronic.

**Findings:** Overall, EBSA had not ensured that its EFAST contractor met the required data accuracy standards. EFAST data from Form 5500s filed on paper, which accounted for about 99 percent of the data, had not consistently met all the accuracy standards EBSA established. Thus, the overwhelming majority of the data were subject to a level of errors that were unacceptable under the terms of the EFAST contract. Our audit did disclose, however, that data from electronically filed Form 5500s met the data accuracy standards. In fact, our statistical sample did not find any errors in electronically filed data. However, since this data only comprised about 1 percent of the data, it did not allow the EFAST data to meet data accuracy standards overall.

As a result, user agencies had to spend resources adjusting and correcting data. While this did not prevent the agencies from accomplishing their missions, it caused them to unnecessarily use resources and prompted the agencies to use alternative methods to accomplish their objectives. In addition, incorrect plan data may have a negative impact on IRS and EBSA enforcement efforts. Errors in such information as type of plan or a dollar amount could prevent a plan from being included in a targeting process or being identified as a high risk.

We found electronic filings processed by EFAST were significantly more accurate than the paper filings processed by the system. In addition, electronic filings were much less expensive to process than paper filings. Using EFAST contract prices for Option Year VI (July 1, 2004 through June 30, 2005), we estimated that if EBSA required all plans to file electronically, it could save over \$5 million annually in contract costs. The combination of increased accuracy at a much lower cost supported EBSA mandating electronic filing of Form 5500s, and the development of a new Form 5500 processing system.

**Recommendations:** We recommended the Assistant Secretary for Employee Benefits Security mandate electronic filing of the Form 5500, consider

## Employee Benefit Plan Annual Reports

---

### **6. Mandate Electronic Filing of Annual Reports by Employee Benefit Plans**

withholding payment to the EFAST contractor if accuracy standards were not met, and include in future EFAST systems development contracts, specific remedies for noncompliance with data accuracy standards.

**Status:** EBSA has published a regulation (29 CFR 2520.104a-2) requiring electronic filing of Form 5500 for plan years beginning on or after January 1, 2008. Since the time of our audit, EBSA officials state that the EFAST contractor has met or exceeded all accuracy standards and, therefore, no penalties have been required. EBSA is continuing its system development efforts for the new EFAST2 system for processing Form 5500s; however, no contract has yet been awarded.

**Report:** 09-05-002-12-121, issued September 30, 2005

# Unemployment Insurance

---

## 7. Work Toward Legislative Change to Require Employers to Report a New Hire's First Day of Earnings

**Summary of Audit:** We conducted a performance audit of the implementation of the New Hire detection method, which is a recent addition to the Unemployment Insurance (UI) Benefit Payment Control methodologies for detecting overpayments. Our objectives were to determine: (1) if New Hire detection was more effective and efficient than the traditional Wage/UI Benefit crossmatch, and (2) what obstacles were preventing states from embracing this detection method.

**Findings:** In response to our questionnaire, 41 states that use New Hire detection indicated that the New Hire detection method is better at detecting UI overpayments earlier than the traditional Wage/UI Benefit Crossmatch. Although more overpayments were identified through New Hire detection as compared to the Wage/UI Benefit Crossmatch methodology, the dollar amount was less because overpayments were detected earlier. In contrast, the overpayments for Wage/UI Benefit crossmatch were higher because it took longer to detect and stop overpayments.

We also concluded that more detailed employer reporting of new hire information to the Department of Health and Human Services (DHHS), which maintains the National Directory of New Hires (NDNH), would further improve the effectiveness and efficiency of New Hire detection. Specifically, employers currently are required to report a new hire within 20 days of the hire date. This 20-day window requires State UI agencies to follow up with the employer to determine how much the employee earned during that period. However, if employers were required to also provide the exact date on which the employee first earned wages, State UI programs would be able to better target their overpayment detection activities.

**Recommendations:** We recommended DOL work with DHHS to communicate to Congress the need for legislative change to require employers to report a new hire's first day of earnings.

**Status:** The Department agreed with this recommendation and stated that in the course of its discussions with DHHS concerning states' access to the NDNH, DOL would explore the potential and implications of seeking legislation to require employers to report a date of first earnings for new hires. We understand OMB intends to pursue necessary changes to enhance New Hire reporting to improve its usefulness in determining eligibility for the UI program.

**Report:** Report No. 05-04-002-03-315, Issued September 30, 2004



# Unemployment Insurance

---

## **8. Analyze and Address the Causes of Unemployment Insurance Overpayments Identified Through the Benefit Accuracy Measurement Program**

**Summary of Audit:** In response to concerns about the accuracy of paid unemployment insurance (UI) claims, in 1987 the Employment and Training Administration (ETA) implemented the Benefit Accuracy Measurement (BAM) program to monitor the accuracy of UI payments made to claimants and statistically project the amount of claimant overpayments throughout the country. Based on statistical projections, BAM estimated UI benefit overpayments of \$2.5 billion for CY 2001 and \$3.7 billion for CY 2002. The OIG audited ETA's use of BAM data to oversee UI overpayments.

**Findings:** As designed, BAM accurately detected and reported overpayments; however, we found that preventing UI overpayments was not a priority of the UI performance management system. Although, over a 12-year period (1989-2001), national overpayment rates reported by BAM ran flat at about 8.5 percent, we determined no corrective actions were taken during this period. We found that ETA did not have effective quality controls in place to prevent overpayments. Poor performance was not identified due to a lack of state-to-state comparisons, and national policies addressing overpayments were not established. ETA's BAM Quality Control Monitoring Handbook defined three distinct regional responsibilities pertaining to Quality Control as program leadership, technical support, and monitoring. However, we concluded responsibilities such as reviewing quality control data to identify factors adversely affecting payments, recommending program improvement studies, and performing data extraction and analysis to identify areas of problems within states were not aspects of monitors' duties. Because of a lack of emphasis by ETA, states did not make overpayments a top priority, as evidenced by State Quality Service Plans (SQSPs) that did not address ways to monitor and prevent overpayments.

**Recommendations:** We recommended that ETA include BAM overpayment analysis in the annual SQSP process, and specifically that ETA negotiate overpayment issues with states to ensure problems are addressed in SQSPs.

**Status:** ETA stated that State and regional office staff negotiated the substance of the SQSPs, but acknowledged that regional office staff did not conduct the analyses recommended in the BAM Handbook. ETA believed it was more efficient for national office staff to continue to provide states and regional offices with analyses about overpayment rates and causes than for the regional offices to engage in overpayment analyses at that level. However, ETA has advised us that its regional offices are now providing overpayment oversight through the SQSP process. This recommendation remains open subject to our verification of ETA's reported corrective actions.

# Hurricanes Katrina and Rita

---

## 9. Tighten Controls Over Disaster-related Unemployment Benefits

**Summary of Audits:** Individuals who were unemployed as a result of Hurricanes Katrina and Rita could claim benefits under one of two unemployment compensation programs delivered by State Workforce Agencies (SWAs) in partnership with DOL's Employment and Training Administration (ETA): State Unemployment Insurance, and Disaster Unemployment Assistance (which is funded by the Federal Emergency Management Agency). To determine if unemployment benefits reached eligible recipients as intended, the OIG initiated audits of Hurricane-related payments made under the two programs.

**Findings:** Our overall finding was that some States relaxed or waived existing controls or utilized new technology without putting compensating controls in place. For example, Louisiana and Mississippi suspended controls over initial eligibility procedures for Disaster Unemployment Assistance (DUA) benefits, which resulted in possible overpayments exceeding \$100 million. Also, Louisiana used debit cards -- a new, untested benefit delivery method -- which lacked proper controls and created opportunities for fraud. Further, Louisiana did not utilize available tools, including Social Security Administration data and the National Directory of New Hires, to verify claimants' identities and screen for claimants who continued to draw benefits despite obtaining employment.

**Recommendations:** We recommended that ETA monitor Louisiana and Mississippi's overpayment collection efforts. We also made several recommendations related to our findings regarding Louisiana's use of debit cards, and its failure to utilize Social Security data and the National Directory of New hires to prevent and detect overpayments.

### Estimated Monetary Benefits:

Mississippi DUA	\$25.1 million
Louisiana DUA	\$62.1 million
Louisiana Debit Cards	\$ 1.2 million
Social Security Verification	\$ 1.1 million
National Directory of New Hires	\$51.2 million

**Status:** ETA has taken action to resolve the audit recommendations; we are continuing to work with ETA to ensure overpayments are collected; adequate controls are in place in Louisiana, internally as well as with contracted service organizations, to safeguard debit cards and protect confidential information belonging to claimants; and data matching with the National Directory of New Hires is implemented by Louisiana and other states.

**Reports:** 06-07-002-03-315, issued September 28, 2007  
06-07-003-03-315, issued September 28, 2007  
06-07-001-03-315, issued March 6, 2007  
06-07-004-03-315, issued September 28, 2007  
06-07-005-03-315, issued September 28, 2007

# **Employment Discrimination Against Veterans**

---

## **10. Conduct More Timely Investigations of Veterans' Employment Discrimination Complaints**

**Summary of Audit:** OIG conducted a performance audit to determine whether the Employment Standards Administration's (ESA) Office of Federal Contract Compliance Programs (OFCCP) was fulfilling its enforcement responsibilities regarding complaints filed by veterans under the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (VEVRAA) alleging discrimination on the basis of their veteran status. VEVRAA prohibits discrimination and requires affirmative action in all personnel practices for special disabled veterans and Vietnam Era Veterans who served on active duty during a war or in a campaign or expedition for which a campaign badge has been authorized.

**Findings:** While we concluded that OFCCP had done an adequate job, overall, in investigating veterans' complaints and evaluating compliance activities of employers that have contracts with the Federal Government, we found that OFCCP was not completing its investigations timely. OFCCP's Federal Contract Compliance Manual called for Area Offices/Field Offices to complete investigation within 60 days after receiving a complaint from the Regional Office; however, we found that district/area offices took an average of 223 days to complete investigations. We also found that OFCCP did not always contact complainants to discuss its findings prior to the conclusion of its investigation, in accordance with its Customer Service Plan.

**Recommendations:** We recommend that OFCCP develop methods to reduce the process time it takes to complete investigations under VEVRAA, and afford each complainant an opportunity to discuss the findings in his/her case prior to the conclusion of the investigation.

**Status:** ESA officials state that a directive addressing processing times for completing investigations and discussing findings with complainants prior to closing investigation should be cleared by the close of FY 2008.

**Report:** 05-02-004-04-410, issued March 29, 2002

# **Workforce Investment Act**

---

## **11. Seek Support for Changes to Workforce Investment Act Training Provisions**

**Summary of Audit:** The Office of Inspector General (OIG) assessed training activities for Workforce Investment Act (WIA) Program Year 2000 Adult and Dislocated Worker programs in selected states. Our objective was to determine the impact of WIA training provisions on program participants, particularly as related to Individual Training Account and Eligible Training Provider systems.

**Findings:** Overall, we found WIA participants generally received appropriate assistance and training options. However, the numbers of WIA participants trained declined as compared to WIA's predecessor program, the Job Training Partnership Act. A number of factors contributed to these declines, including some states' slow progress in implementing WIA. Many states struggled with training provider eligibility. Many training providers found WIA reporting requirements burdensome – and considered discontinuing their participation -- because they had to report outcomes for both WIA and non-WIA students. Some local workforce boards interpreted WIA as requiring "Work-First," which resulted in their directing participants to job search and other activities instead of training. Finally, some training providers were hesitant to disclose participant data necessary for WIA performance reporting and determination of providers' subsequent eligibility for fear of violating the education privacy statutes.

**Recommendations:** We recommended the Department seek support for changes in WIA's provisions to encourage training provider participation; reduce eligible training providers' reporting burden associated with reporting data on non-WIA students and support amendments to legislation that will eliminate uncertainty regarding liability for the release of personal identifying information for WIA reporting purposes; and

**Status:** The Department has stated that implementation of the OIG's recommendations depends on the outcome of the ongoing effort to reauthorize WIA, whose authorization expired September 30, 2003.

**Report:** 04-03-017-03-390, issued March 31, 2003

## **Discretionary Grants**

---

### **12. Document All Decisions and Discussions That Lead to Actions by DOL Officials That Affect How and to Whom Grant Funds Are Distributed**

**Summary of Audit:** We conducted an audit to determine if proper procurement procedures were followed in awarding non-competitive grants under the Department's High Growth Job Training Initiative (HGJTI). HGJTI is a strategic effort to prepare workers to take advantage of new and increasing job opportunities in high-growth, high demand, and economically vital sectors of the American economy. The purpose of HGJTI is to target education and skills development resources toward helping workers gain skills needed to build successful careers in these and other growing industries. During the period July 1, 2001, through March 31, 2007, the Employment and Training Administration (ETA) awarded 157 HGJTI grants totaling \$271 million. Of this amount, ETA accepted unsolicited proposals and awarded 133 grants totaling \$235 million (87 percent) through non-competitive procurement methods.

**Findings:** We found that ETA could not demonstrate that it followed proper procurement procedures in 35 of 39 tested non-competitive awards (90 percent). These 35 awards totaled \$57 million. Specifically, decisions to award 10 non-competitive grants were not adequately justified, reviews of unsolicited proposals were not consistently documented, and matching requirements of \$34 million were not carried forward in grant modifications. These failures to follow proper procurement procedures resulted from a control environment that did not ensure adherence to applicable criteria, nor that decisions to award grants non-competitively were adequately documented. ETA could not demonstrate that it made the best decisions in awarding grants to carry out HGJTI. Further, since matching requirements were not carried forward in some grant modifications, the programs and levels of services provided could be significantly reduced from those intended in the original grants.

**Recommendations:** We made eight recommendations to the Assistant Secretary for Employment and Training to improve management controls over grant awards. In summary, we recommended the Assistant Secretary take steps to ensure: competition is encouraged for discretionary grant awards; award decisions are adequately documented; and matching requirements of \$34 million are carried forward in grant modifications.

**Status:** The Assistant Secretary for Employment and Training strongly disagreed with our findings related to the procurement practices utilized for non-competitive grants. The Assistant Secretary stated that sufficient documentation had been provided to support that the awards met departmental policy regarding non-competitive procurement. ETA further stated that there were no specific requirements to document procurement decisions.

## **Discretionary Grants**

---

### **12. Document All Decisions and Discussions That Lead to Actions by DOL Officials That Affect How and to Whom Grant Funds Are Distributed**

Proper stewardship of Government funds necessitates maintaining documentation sufficient to demonstrate that funds were properly expended regardless of any explicit requirement to do so. In 2005, we conducted an audit to assess the propriety a \$1.1 million contract that Chinatown Manpower Project, Inc., received under a \$25 million Workforce Investment Act National Emergency Grant (NEG) that the U. S. Department of Labor (Department) awarded the New York State Department of Labor (NYSDOL) after the September 11, 2001, attack on the World Trade Center (WTC). We found that the Department was substantially involved in arrangements to provide funding for CMP's subcontractors. The Department's actions led NYSDOL to believe the Department had sanctioned specific organizations to receive the \$1 million earmarked for Chinatown, which in turn led CMP to enter into subcontracts with those organizations without full and open competition. We also found that the Regional Representative in New York created an appearance of favoritism because she had long-term friendships with executives of two of the selected organizations. We recommended that a record be maintained of decisions and discussions that lead to actions by departmental officials that affect how and to whom grant funds are distributed. In response to our report, the then-Deputy Secretary of Labor stated that ETA had implemented enhanced recordkeeping to promote transparency in the grant making process.

Despite this assurance in response to the findings of our audit of Chinatown Manpower, ETA's response to our audit of HGJTI grant awards asserts there is no requirement to document procurement decisions. This change in position by ETA evidences a control environment that does not emphasize adherence to applicable procurement criteria, or the need to adequately document decisions to award grant funds. Nonetheless, ETA recently updated the status of their planned corrective actions and stated that all actions would be completed by January 31, 2008. The OIG will verify ETA's actions.

Reports: 02-08-201-03-390, issued November 2, 2007  
02-05-202-01-001, issued August 24, 2005

## Job Corps

---

### 13. Strengthen Efforts to Identify Students with Unknown or Undisclosed Cognitive Disabilities

**Summary of Audit:** OIG conducted a performance audit to evaluate Job Corps' processes for assessing students for unknown or undisclosed cognitive disabilities, such as learning disabilities, attention deficit hyperactivity disorder, mental retardation, and traumatic brain injury. Job Corps is a \$1.2 billion educational and vocational training program (primarily residential) for economically disadvantaged youth ages 16 through 24 who often face multiple barriers to gainful employment. This program provides career counseling, technical skills and academic training, social education, and other support services to more than 60,000 individuals annually at 126 centers nationwide. Studies suggest certain characteristics, e.g., high school drop out, below eighth grade reading level, and never held a full-time job, are prevalent in both cognitively disabled youth and Job Corps' student population. It is likely that a disproportionate number of individuals with cognitive disabilities enroll in alternative training programs, such as Job Corps, due to their high failure rates in the public school sector and high unemployment rates.

**Finding:** We found that improving efforts to assess and account for students with unknown or undisclosed cognitive disabilities would help Job Corps achieve its overall mission. Although Job Corps is not legislatively required to specifically assess all students for cognitive disabilities, doing so would help Job Corps achieve its program goals of improving educational achievements of Job Corps students and increasing participation of Job Corps graduates in employment and education. Effective identification and accommodation of students with cognitive disabilities would address significant barriers to employment and improve the program's student outcomes.

**Recommendations:** We recommended that (1) Job Corps conduct a pilot program to develop an appropriate and cost effective screening and formal evaluation methodology to identify students with unknown or undisclosed cognitive disabilities, and (2) based on the pilot program's results, develop and implement national policies and procedures as needed to screen all students for cognitive disabilities and obtain formal evaluations when screening indicates a potential cognitive disability.

**Status:** Job Corps opposes expending funds on a new screening and formal evaluation program that it believes has no solid basis in the current scientific research. Alternatively, Job Corps stated that it has updated and strengthened its policies and technical guidance for identification of cognitive disabilities, continued to follow the research concerning proposed new models and strategies for identifying cognitive disabilities, and strengthened its site-level systems such as staff training, technical guidance and monitoring to ensure that students with cognitive disabilities are identified and assessed.

## **Job Corps Performance Data**

---

### **14. Improve Monitoring of Job Corps Performance Data**

**Summary of Audits:** The OIG conducted nine performance audits that reviewed aspects of Job Corps reported performance data. Those audits identified deficiencies primarily in student accountability (attendance and leave), On-board Strength (OBS), and student accomplishments (e.g. vocational completions). Our audits identified manipulated or incomplete training records that contradicted reported performance outcomes such as vocational completions, General Education Development (GED) Certificates, and High School Diplomas. We also found unsigned resignation forms. In addition, some Center Directors reported placement outcomes that were either invalid or unreliable. Additionally, we noted that manipulations of performance data also negatively impacted the reporting of weekly termination rates (WTR), and 30-day and 60-day commitment rates. Further, we identified significant management control weaknesses in onsite assessments performed by Job Corps Regional Offices that included weaknesses in the validation of performance data.

**Findings:** Our summary finding was that some Center Directors used various leave categories and undated resignation forms to extend the stays of students beyond their required termination dates. Those leave categories included absent without leave, present for duty off center, and unpaid administrative leave. In addition, we identified weaknesses in performance data for placement outcomes and vocational completions that were either invalid or unreliable. Also, center personnel engaged in practices that improperly inflated OBS by allowing students who incurred excessive absences without leave to remain in the program. These actions resulted in the assessment of liquidated damages and the underutilization of facility capacity, estimated at almost \$2 million as follows:

**Estimated Monetary Benefits:**

Liquidated Damages (Laredo JCC)	\$ 96,962
Liquidated Damages (Grafton JCC)	\$ 56,824
Liquidated Damages (Cincinnati JCC)	\$ 201,121
Underutilization of Facility Capacity (Oconaluftee JCC)	\$ 190,367
Liquidated Damages (San Diego JCC)	\$ 616,369
Liquidated Damages and Incentive Fees (Kittrell JCC)	\$ 776,000
<b>Total</b>	<b><u>\$1,937,643</u></b>

**Recommendations:** We recommended that the National Director, Office of Job Corps require Center directors to comply with requirements to timely terminate students who exceed absence limitations and collect the reported liquidated damages. We also recommended that controls be strengthened at centers and that Job Corps Regional Offices increase monitoring of centers, verify center reported performance data, and document the methods used and conclusions drawn from efforts made to validate performance data.

**Status:** The National Director, Office of Job Corps has taken action to resolve the audit recommendations; we are continuing to work with Job Corps towards



## Job Corps Performance Data

---

### 14. Improve Monitoring of Job Corps Performance Data

closing recommendations to monitor and verify that Center operators and other contractors have strengthened controls to ensure proper recording of student attendance, student leave, vocational completions, and job placements.

**Reports:** 09-07-002-01-370; issued September 28, 2007  
09-07-004-01-370; issued September 28, 2007  
03-07-003-01-370; issued March 30, 2007  
26-07-001-01-370; issued March 30, 2007  
09-06-004-01-370; issued September 29, 2006  
09-05-004-03-370; issued September 30, 2006  
09-05-001-03-370; issued March 30, 2006  
09-04-004-03-370; issued September 30, 2004  
09-04-007-03-370; issued November 28, 2003

## **Procurement (cross-cutting recommendations)**

---

### **15. Create Organizational Separation Between DOL Procurement and Program Functions**

**Summary of Audits:** The OIG conducted two audits that made high-level recommendations regarding the organizational placement of procurement functions in the Department of Labor. The first was an audit in response to a series of allegations we received regarding procurement and contracting procedures, Government travel and purchase card usage, computer security, and personnel issues in DOL's Mine Safety and Health Administration (MSHA). The objective of our audit was to determine the merits of the allegations and, for those that had merit, recommend appropriate corrective action.

The second unrelated audit was in response to allegations received, as well as a referral from DOL's Assistant Secretary for Administration and Management, about a contract awarded by DOL to the Meganet Corporation for the purchase of encryption software and services.

**Findings:** In the MSHA audit, we found that a lack of segregation of the procurement function allowed program staff to exert undue influence over the procurement process. In addition, we found the agency's procurements exhibited a pattern of disregard for acquisition requirements and did not adhere to the principle of full and open competition. By operating in such an environment, management was unable to ensure that contracts were in the best interest of the Government, and that all eligible contractors were given the opportunity to compete for the agency's contracts.

Our audit of the Meganet contract disclosed that overall responsibilities for the information technology and procurement functions were delegated to one executive. Further, a program official from that agency who was involved in the procurement action failed to disclose an apparent conflict of interest. The audit also found: the noncompetitive award was not adequately justified; the contract was significantly modified in scope and cost without proper review and approval; and the agency could not justify its decision not to use the \$3.8 million of products purchased.

**Recommendations:** In the MSHA audit, our sole recommendation was that the Deputy Secretary of Labor direct the DOL Procurement Executive to rescind MSHA's procurement authority, reassign such authority, and ensure that it is completely independent of MSHA.

---

Our overarching recommendation in the Meganet audit was that the Deputy Secretary remove the procurement function from the Office of the Assistant Secretary for Administration and Management and create an independent Acquisition Office that would report directly to the Deputy Secretary.

**Status:** The Department has neither agreed to nor implemented the OIG's recommendations. Further, for the past 3 years, the OIG has identified the lack

## **Procurement (cross-cutting recommendations)**

---

### **15. Create Organizational Separation Between DOL Procurement and Program Functions**

of segregation of procurement duties as a Top Management Challenge for DOL. In particular, we have noted that the Services Acquisition Reform Act of 2003 (SARA) requires that executive agencies appoint a Chief Acquisition Officer (CAO) whose primary duty is acquisition management. In January 2007, the Secretary of Labor issued Order 2-2007, which formally established the position of CAO within DOL and specifically stated that the CAO would have acquisition management as his or her primary duty. However, the Department's current organization is not in compliance with this requirement, as the Assistant Secretary for Administration and Management is serving as the CAO while retaining other significant non-acquisition responsibilities. The OIG has called on the Department to move expeditiously to implement the Secretary's Order, comply with SARA requirements, and separate the procurement and program functions as the OIG has recommended.

**Report:** 25-05-001-06-001, issued October 29, 2004  
05-05-005-07-720, issued March 31, 2005

## Information System Security

---

### **16. Remedy Information Security Control Weaknesses That Could Compromise Information or Result in Disruptions in the Delivery of Program Services**

**Summary of Audit:** The Federal Information Security Management Act requires the OIG to perform annual independent evaluations of DOL's information security program and practices. In carrying out its mission to foster and promote the welfare of job seekers, wage earners, and retirees, DOL administers a variety of Federal labor laws, including those that guarantee workers' rights to safe and healthful working conditions, a minimum hourly wage and overtime pay, freedom from employment discrimination, unemployment insurance, and other income support. DOL's information systems play a vital role in producing key economic indicators, ensuring workers' safety and health, and paying billions of dollars in unemployment and other benefits.

**Findings:** We found significant deficiencies related to access controls across DOL financial and non-financial information systems, and that DOL had not fully implemented OMB's government-wide requirements to protect personally identifiable information. If access to the systems we tested was compromised and the systems were to become unavailable, DOL would be unable to deliver program services.

**Recommendations:** We issued over 200 recommendations to DOL agencies in FY 2007 dealing with compliance with minimum system security requirements. In addition, we recommended that the Department's Chief Information Officer take the following actions related to the identified significant deficiencies: (1) implement an enhanced Department-wide monitoring program, to include appropriate testing and monitoring, that is sufficient to afford management reasonable assurance of compliance with DOL's access controls policies and procedures; and (2) work with the [redacted] to establish an information security program, to include appropriate testing and monitoring, that is designed to afford management reasonable assurance of compliance with DOL security policies and procedures. Finally, we recommended that the Chief Information Officer implement an enhanced Department-wide monitoring program, to include appropriate testing and monitoring, that is sufficient to afford management reasonable assurance of compliance with DOL's access controls policies and procedures.

**Status:** The Office of the Chief Information Officer has established a corrective action plan to address our recommendations. We have initiated followup work to determine whether DOL agencies are correcting the identified security vulnerabilities.

**Report:** 23-07-004-07-001; Issued September 28, 2007

## Unemployment Insurance Disaster Recovery Plans

### **17. Ensure that Contingency Planning Weaknesses in State Workforce Agencies' Unemployment Systems are Corrected to Prevent the Disruption of Benefits to Unemployed Americans**

**Summary of Audits:** Enacted more than 65 years ago as a Federal-state partnership, the Unemployment Insurance (UI) program is the Department's largest income maintenance program. This multibillion-dollar program provides income maintenance to individuals who have lost their jobs through no fault of their own. While the framework of the program is determined by Federal law, UI benefits are paid directly by the states. Therefore, the Department must be able to ensure the states have a secure and viable mechanism in place to make payments. The Information Technology (IT) contingency plans for selected State UI systems have been reviewed by the Office of Audit through several audits over the past decade. These audits were conducted in response to Employment and Training Administration (ETA) requests and performed in accordance with the Federal Information Security Management Act (FISMA).

**Finding(s):** In 1998, OIG performed a review of the vulnerability of the state UI programs and their planned readiness to overcome threats. This work resulted in identifying that 30 out of 53 UI jurisdictions were vulnerable. In addition, OIG conducted nine FISMA audits of state UI systems between Fiscal Year (FY) 2001 and FY 2005 and identified that seven of the nine states' UI systems exhibited one or more high-risk weaknesses in relation to contingency planning during the audited period. The high-risk weaknesses included incomplete and untested contingency plans.

**Recommendation(s):** No recommendations were issued related to the 1998 audit. During FY 2001 through FY 2005, IG issued 18 recommendations to the States directing them to finalize their contingency plans and to regularly conduct tests of those plans.

**Status:** The nine audited states have submitted information to ETA stating that they have taken corrective action. We are currently conducting a followup audit in [ ] that will assess the adequacy of [ ] contingency plans. 62

**Reports:**

23-02-008-03-315;	issued September 13, 2002
23-02-009-03-315;	issued September 13, 2002
23-03-003-03-315;	issued March 11, 2003
23-03-005-03-315;	issued February 27, 2003
23-04-016-03-315;	issued September 30, 2004
23-04-017-03-315;	issued September 30, 2004
23-04-018-03-315;	issued September 30, 2004
23-05-007-03-315;	issued September 30, 2005
23-05-019-03-315;	issued September 30, 2005

## Protection of Personally Identifiable Information

### **18. Implement Information Security Controls to Reduce the Risk of Exposing Personally Identifiable Information to Unauthorized Access and Use**

**Summary of Audits:** Following numerous incidents involving the compromise or loss of sensitive personal identifiable information (PII), the Office of Management and Budget (OMB) issued Memorandum M-06-16, *Protection of Sensitive Agency Information*, on June 23, 2006. The memorandum stated that Federal Agencies needed to take all necessary and reasonable measures to swiftly eliminate significant vulnerabilities to the sensitive information entrusted to them. It required Agencies to take certain actions by August 7, 2006, to ensure that safeguards were in place and appropriately reviewed. As required by OMB M-06-16, we completed an evaluation of the Department's actions in response to OMB M-06-16, and we have subsequently conducted additional information security audit work related to protecting PII.

**Findings:** We found that the Department had partially implemented the National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Security Checklist for protection of [redacted] as well as two of the four specific OMB M-06-16 recommendations which relate to [redacted] and a [redacted]. The remaining two specific OMB M-06-16 recommendations which relate to [redacted] and [redacted] had not been implemented. In addition to the above, another audit found information security weaknesses in the [redacted] that included the ability of users to gain unauthorized access to the [redacted]. These users would have access to PII and the ability to fraudulently add, modify or delete [redacted]. In the [redacted] we found that a remote system database administrator for the [redacted] had unencrypted access [redacted]. This individual was making back-up copies of data and maintaining this information at home on personal equipment. Until the necessary actions to comply with all provisions of M-06-16 and the related NIST controls over protecting PII are implemented, the Department remains at an increased risk of exposing PII to unauthorized access and use. b2

**Recommendations:** We recommended that the Chief Information Officer ensure full Department-wide implementation of the security controls included in the NIST Security Checklist. We also recommended the Department fully implement the four specific OMB M-06-16 recommendations related to encryption of mobile devices, remote access through two-factor authentication, logging of sensitive database extracts, and a 30-minute "timeout" function for remote access and mobile devices.

## Protection of Personally Identifiable Information

### **18. Implement Information Security Controls to Reduce the Risk of Exposing Personally Identifiable Information to Unauthorized Access and Use**

**Status:** The NIST security checklist contains 11 action items to be implemented by the Department to safeguard remote information. As of September 2006, DOL had fully implemented [ ] of the [ ] action items, partially implemented [ ] of the [ ] action items, and had not implemented [ ] action item. Regarding the four specific OMB M-06-16 recommendations, the Department reports that the [ ] has been implemented but awaits OIG verification. [ ] and [ ] are planned to be completed by the first quarter of FY 2009.

According to Agency officials, the [ ] and [ ] vulnerabilities related to PII have been corrected. The OIG is currently performing follow-up work to confirm that the vulnerabilities no longer exist.

**Report:** 23-07-001-07-001, issued March 30, 2007  
23-07-004-07-001, issued September 28, 2007

# 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 incident. [redacted] is the f

[redacted] is often an attempt to [redacted] sensitive information. The user believes the [redacted] to the computer.

The CSI Report identified the [redacted] as using his personal e-mail account to [redacted] the sender.

[redacted] 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 [redacted] violate Department policy in testing the e-mail service with [redacted]

**March 2007**

### COMPUTER SECURITY INCIDENT INVOLVING E-MAIL DISTRIBUTION LIST TESTING

#### WHAT OIG FOUND

We found that the [redacted] actions violated DOL policy when he took it upon himself to [redacted] to test the DOL e-mail service without being authorized to do so. However, he notified responsible agency officials in advance, the [redacted] he sent caused no harm to the DOL and his actions resulted in the discovery of a security vulnerability related to [redacted]

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 [redacted] 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 [redacted] 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

b2 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 [ ] incident. The CSI Report identified the [ ] as using his [ ] b6/b7c

personal e-mail account to [ ] Our [ ] b2

objective was to determine: b6

- Did the [ ] violate Department policy in testing the e-mail service with [ ]

### Results

We found that the ESA [ ] actions violated Department of Labor (DOL) policy when he took it upon himself to [ ] messages to test the DOL e-mail service without being authorized to do so. However, he notified responsible agency officials in advance, the [ ] he sent caused no harm to the DOL e-mail service, and his actions resulted in the discovery of a security vulnerability related to [ ] 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 [ ] 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. b6/b7c

### 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.

**Computer Security Incident Involving  
E-mail Distribution List Testing**

---

**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 [ ] incident that occurred in December 2005. We initiated the audit in response to a CSI Report from OCIO, which identified [ ] as using his personal e-mail account to [ ] b2

[ ] Our objective was to determine:

- Did the [ ] violate Department policy in testing the e-mail service with [ ] b2

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 [ ] violate Department policy in testing the e-mail service with [ ] b6/1c b2

[ ] b6/1c violated Department policy when he took it upon himself to test the -by [ ] -without being authorized to do so. He had previously expressed concern to [ ] that a virus e-mail message had gotten through [ ] and did not believe action was being taken to address this IT security issue. [ ] notified [ ] that he planned to run some tests [ ] and felt this was sufficient authorization for him to go forward. While the [ ] were not damaging to the [ ] their discovery did necessitate an investigation by OASAM IT personnel to determine what had occurred. A positive result of [ ] actions was that he identified a security vulnerability in the [ ] that required corrective action. b2

[ ] 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 [ ] 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 [ ] incident, and are also shown in a timeline at Exhibit A. b2

On November 29, 2005, the [ ] received an e-mail message [ ] Even though the [ ] system [ ] and [ ] the [ ] was [ ] questioned the security policy of the distribution lists to [ ] but was told by an [ ] member that the e-mail message was directed at him and nothing was wrong with the distribution list. b6/1c b2

On December 5, 2005, [ ] learned that [ ] had received the November 29<sup>th</sup> [ ] message. In following up on the matter with [ ] [ ] said he would run some tests [ ] to determine what [ ] were not functioning properly, including whether ESA had configured something incorrectly during the [ ] b2

b2  
[ ] test whether [ ] the [ ]

b6/b7c  
[ ] created [ ]

The recipients were as follows:

• [ ] which was where the [ ] it b2  
[ ] If this was the [ ]  
[ ] would indicate a problem with [ ]

• [ ] If this [ ] and the one to the [ ] b2  
[ ] went through, it would indicate controls related to the [ ]  
[ ] were not configured correctly to handle [ ]

• [ ] If this [ ] b2  
[ ] It would indicate [ ]  
[ ] were not configured correctly to [ ]

After [ ] messages, the [ ] signed onto his [ ] b2  
[ ] account and found that [ ] thereby showing [ ]  
[ ] vulnerabilities at [ ]

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 [ ]  
e-mail administrator notified the ITC Help Desk of the [ ] incident and that [ ] b2  
there were security issues related to [ ]

b6/b7c [ ] actions caused no harm to the [ ] and resulted in the [ ]  
[ ] discovery of a security vulnerability related to [ ] However, in [ ] b2  
[ ] 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. [ ] resolved the issue on the [ ] b2

[ ] and a senior OASAM official told us that [ ] plans [ ]  
[ ] to request that [ ]  
[ ] Regardless of the resultant positive  
impact, actions such as those taken by [ ] 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.





## **Exhibit**

---

[THIS PAGE INTENTIONALLY LEFT BLANK]

**Timeline:**

- 7:15 am [ ]
- 8:29 am & 8:38 am [ ] email [ ]  
distribution list but simply an email directed at him
- 11:01 am [ ]  
Original transmission of [ ]  
learns [ ]
- 2 pm [ ] some tests [ ] talks to [ ]
- 2:28 pm & 8:39 pm [ ] management teams of his actions
- 9:35 pm & 9:38 pm [ ] JTC Acting Operations Director recognizes [ ]  
Technical Announcements and begins investigation
- 8:36 am [ ] ESA Email Administrator emails [ ]  
Help Desk has been informed of the incident.
- 12:57 pm [ ] JTC Acting Operations Director talks to [ ] confirming the details  
of the incident.

11/29/2005      12/05/2005      12/06/2005

[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 [ ] which incorporated knowledgeable staff from the various component agencies. [ ] 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 [ ] b2

ESA maintains its own computers and networks that connect to OASAM's network. The group responsible for ESA computers and networks is the [ ]



[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 [ ] by the [ ] through the Department's [ ]. The objective of our audit was to determine:

- Did the [ ] violate Department policy in testing the e-mail service with [ ]

**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 [ ] 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 [ ]. We developed a timeline using information from these interviews, and recreated, in a test environment, the steps involved to perform the [ ]. 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
ESA	Employment Standards Administration
IT	Information Technology
ITC	Information Technology Center
OASAM	Office of Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

[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.