

Office of Inspector General

U.S. Department of Labor
Office of Audit

**CONTROLS OVER THE DISCLOSURE, ACCESS,
AND USE OF
SOCIAL SECURITY NUMBERS IN THE
FEDERAL EMPLOYEES COMPENSATION ACT PROGRAM
EMPLOYMENT STANDARDS ADMINISTRATION
FEBRUARY THROUGH AUGUST 2002**



**Report Number: 03-03-002-04-001
Date Issued: December 20, 2002**

TABLE OF CONTENTS

ACRONYMS..... ii

EXECUTIVE SUMMARY 1

BACKGROUND 4

OBJECTIVES, SCOPE, AND METHODOLOGY..... 7

AUDIT RESULTS, FINDINGS, AND RECOMMENDATIONS 9

 1. The Standard Claim Forms Need to be Revised10

 2. A Cost-Effective Plan for Onsite Monitoring of Contractors and Other Entities
 Needs to be Implemented12

 3. Controls over the Release of Records to
 Noncontractor Physicians Need to be Improved14

AGENCY’S RESPONSE TO DRAFT REPORT16

ACRONYMS

CIO	Chief Information Officer
DFEC	Division of Federal Employees Compensation
DLMS	Department of Labor Manual Series
DOL	U.S. Department of Labor
ESA	Employment Standards Administration
FECA	Federal Employees' Compensation Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	General Accounting Office
IME	Independent Medical Examination
OIG	Office of Inspector General
OWCP	Office of Workers' Compensation Program
PCIE	President's Council on Integrity and Efficiency
SSA	Social Security Administration
SSN	Social Security Number
USC	United States Code

EXECUTIVE SUMMARY

The Social Security Number (SSN) was created in 1936 as a means of tracking workers' earnings and eligibility for social security benefits. Over the years, the SSN has become a *de facto* national identifier used by Federal agencies, state and local governments, and private organizations. In recent years there have been concerns related to perceived widespread sharing of personal information and occurrences of identity theft. Therefore, the chairman of the House Ways and Means Subcommittee on Social Security requested the Social Security Administration's (SSA) Office of Inspector General (OIG) and the President's Council on Integrity and Efficiency (PCIE) to determine, across government, the methods Federal agencies use to disseminate and control the SSN. The PCIE, through the SSA/OIG, requested the OIG PCIE members to perform an audit of controls over the disclosure, access, and use of SSNs in one of their department or agency programs.

Using instructions provided by the SSA/OIG and the PCIE, we assessed the relative risks of improper disclosure, access, and use of SSNs for the five programs identified by DOL as collecting the largest number of SSNs. Based on our assessment, we selected the U.S. Department of Labor's (DOL) Federal Employees' Compensation Act (FECA) program for our audit. The Employment Standards Administration's (ESA) Office of Workers' Compensation Programs (OWCP) administers FECA. OWCP's Division of Federal Employees' Compensation (DFEC) is responsible for managing FECA programs.

The overall audit objective was to assess DFEC's management controls over the disclosure, access, and use of SSN information by third parties. Our specific audit objectives were to determine if DFEC: (1) has adequate controls to ensure legal and informed disclosures to third parties; (2) has adequate controls over contractors, and other entities, who have access and use of SSNs; and (3) has adequate controls over access to SSNs maintained in its databases.

To perform our audit, we followed the procedures in an audit guide provided by the SSA/OIG. To accomplish the audit we interviewed DFEC officials, reviewed policies and procedures relevant to the audit objectives, visited the FECA central mail facility, and considered the results of an OIG audit on general controls and security over selected financial management systems, which included the Federal Employees' Compensation System. The SSA/OIG audit guide did not require, nor did our audit include, testing the effectiveness of DFEC controls over the disclosure, access, and use of SSNs. We conducted our fieldwork from February to August 2002.

Overall, our audit determined that management controls within the FECA program, if followed, provide reasonable assurance that legal and informed disclosure is taking place, and adequate controls exist over the access and use of SSNs by contractors and other entities. Our examination of third parties' contracts disclosed that appropriate security procedures exist for safeguarding SSNs, and the contracts do include the Privacy Act notification. We

also determined that adequate controls exist over the access and use of SSNs in DFEC's automated databases.

However, we noted several opportunities for OWCP to improve existing DFEC controls over SSNs for FECA. Specifically, we found:

1. Standard forms used for claims do not directly associate the claimant's signature with his or her acknowledgement of the Privacy Act Disclosure Statement. The multiple-page form requires the claimant's signature on the first page; however, the Privacy Act Disclosure Statement does not appear until the last page. Since the other pages are completed by individuals other than the claimant, questions could be raised about whether the claimant was aware that disclosures of information on the form to third parties could occur.
2. Limited onsite monitoring is done of contractors and other entities that have access to claimant files containing SSNs. Instead of onsite monitoring, DFEC relies on the training it provides to the contractors as part of the certification process. However, without sufficient onsite monitoring, DFEC cannot ensure that contractors and others are complying with security and disclosure requirements.
3. DFEC is not consistently providing physicians, who do not have contracts or agreements with DOL, adequate notification of their responsibilities to comply with Privacy Act requirements when they are provided FECA claimant case files. Additionally, we were told about instances in which claimant files provided to physicians conducting independent medical examinations (referred to as Independent Medical Examination (IME) physicians) have either been lost or returned with missing documents.

To improve controls over DFEC's use and security of SSNs, we recommend that the Assistant Secretary for Employment Standards require OWCP to:

1. Revise the standard claimant forms to ensure that the claimant is aware of the Privacy Act Disclosure Statement.
2. Develop and implement a cost-effective, onsite monitoring program that will provide reasonable assurance that contractors and other entities are complying with the requirements for safeguarding the access and use of FECA claimants' SSNs.
3. Provide second opinion and IME physicians a cover letter when providing them claimant files or documentation, explaining in detail the physicians' responsibility to comply with Privacy Act requirements.
4. Explore the extent and cause of losses of claimant files or documents by IME physicians and take any necessary corrective action.

Our conclusions and recommendations are valid only with regard to the management controls over FECA as they existed during the period of the audit, February to August 2002. Projection of the adequacy of FECA management controls to future periods is subject to the risk that those controls may become inadequate because of changes in conditions, or that the effectiveness of the design and operation of policies and procedures may deteriorate.

In response to the draft report, the Assistant Secretary for Employment Standards generally agreed with the findings and recommendations. The recommendations can be resolved when ESA provides the planned dates for achieving the corrective action. The entire response is included at the end of this report

BACKGROUND

SSA created the SSN in 1936 as a means of tracking workers' earnings and eligibility for social security benefits. Over the years, the SSN has become a *de facto* national identifier used by Federal agencies, state and local governments, and private organizations. Government agencies frequently ask individuals for their SSNs to comply with applicable laws and regulations or to efficiently track and exchange information. A number of laws and regulations impose limitations on how agencies may use SSNs.

Due to concerns related to the perceived widespread sharing of personal information and occurrences of identity theft, the chairman of the House Ways and Means Subcommittee on Social Security requested the SSA/OIG and the PCIE to determine, across government, the methods that Federal agencies use to disseminate and control the SSN. The PCIE, through the SSA/OIG, requested OIG members of the PCIE, including DOL, to participate in an audit of the controls over the disclosure, use, and access of SSNs. The results of the work performed by all the OIGs that participated in this PCIE initiative will be consolidated in a report to be issued by the SSA/OIG.

The Federal Employees' Compensation Act Program

DOL, through ESA, is charged with administering the FECA program. The Federal Employees' Compensation Act, 5 U.S.C. § 8101-8193 (FECA), provides compensation and medical benefits to Federal civilian employees and their dependents for job-related injuries, diseases, or deaths. Within ESA, OWCP's DFEC has the responsibility for establishing policies and procedures for the administration and operation of the FECA program. DFEC has 12 district offices throughout the country to service FECA claimants.

FECA provides workers' compensation coverage to three million Federal and Postal workers around the world for employment-related injuries and occupational diseases. During Fiscal Year (FY) 2000, over 176,000 new cases were opened, and the program provided nearly 273,000 workers more than \$2 billion in benefits for work-related injuries and illnesses. According to DFEC, there were about 360,000 Federal employees' SSNs in its computer system at the end of calendar year 2001.

To claim benefits under FECA, an employee who sustains a work-related traumatic injury or an occupational disease must give notice in writing on Form CA-1 or Form CA-2, respectively. The employee or another person must forward this notice to the employer. According to FECA procedures, it is mandatory that an injured employee provide his or her SSN in order to receive program services.

DFEC assigns the case a primary identification number that is unique to the district office. DFEC uses the claimant's social security number as a secondary identifier. However, various entities outside of DFEC (e.g., other Federal agencies, medical providers, claimants, claimant representatives, etc.) make requests for claimant information using the claimant's name and SSN. The requests are made using the claimant's SSN because it is a unique identifier commonly used by private organizations and Federal, state, and local governments as a method for filing records.

Six types of OWCP contractors used for the FECA program are authorized to have access to claimants' SSNs. The type of contractors and services they provide are:

1. **Nurses.** These contractors assist claimants in person or by telephone in managing the claimant's health issues.
2. **Data Entry.** These contractors provide DFEC district offices with data entry technicians responsible for keying claimant data into various forms and files.
3. **Systems Management.** These contractors are responsible for managing and maintaining the automated data processing system used for the FECA program.
4. **Central and Local Mail.** One contractor operates the DFEC central mailroom and another contractor supplies staff to supplement the Federal staff at the DFEC district office mailrooms. The central mailroom contractor is also responsible for imaging claimant documents into an electronic file.
5. **Rehabilitation.** OWCP has contracts with numerous vocational rehabilitation counselors to transition injured employees from non-working to working status.
6. **Physician Brokers.** These contract physician brokers obtain physicians who provide second opinions to independently determine a claimant's physical or mental status relating to the reported injury/illness. These second opinion physicians are not under contract with OWCP.

The Privacy Act and the Freedom of Information Act (FOIA) establish the framework for restricting SSN disclosure.¹

The Privacy Act. The Privacy Act regulates the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. In particular, the Privacy Act requires that Federal agencies maintaining systems of records containing information of a personal nature and retrieving data by name, or other personal identifying designation (e.g., SSN), establish rules of conduct for employees involved in the design, development, maintenance, or operation of any such system.

¹ Privacy Act (5 U.S.C. § 552a) and Freedom of Information Act (5 U.S.C. § 552).

DOL's Department of Labor Manual Series (DLMS) 5, Chapter 200, prescribes the rules of conduct and responsibilities for DOL employees in the handling of personal information contained in systems of records covered under the Privacy Act of 1974 that are in the custody of the DOL, excluding Civil Service Commission personnel records.

FOIA. The FOIA generally provides that any person has a right to obtain access to Federal agency records, except for those records that are protected from disclosure by nine stated exemptions. Under exemption 6 of the FOIA, the government is permitted to withhold information about individuals in "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

DLMS 5, Chapter 300, interprets the requirements of the FOIA, establishes uniform procedures, and assigns responsibilities for responding to requests for records.

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The overall audit objective was to assess the extent of DFEC's management controls over the disclosure, use, and access of SSN information by third parties. Our specific audit objectives were to determine if DFEC: (1) has adequate controls to ensure legal and informed disclosures to third parties; (2) has adequate controls over contractors, and other entities, who have access and use of SSNs; and (3) has adequate controls over access to SSNs maintained in its databases.

SCOPE AND METHODOLOGY

We selected the FECA program for the audit based on the results of our review of the responses to a questionnaire sent by the General Accounting Office (GAO) to DOL's Chief Information Officer (CIO). GAO requested information on the five largest DOL agencies that routinely collect, maintain, and use SSNs.² We reviewed the responses to the GAO questionnaire to determine which of the five programs appeared to have the highest risk of improper disclosure, access, and use of SSNs. The five DOL programs, all administered by ESA, were: FECA, Black Lung, Longshore, Energy Employees Occupational Illness Compensation and Wage and Hour. The results of our work found no obvious reported weaknesses concerning the security of SSNs for any of the five DOL programs that would cause us to select one program over the other for audit. Therefore, we selected FECA for our audit primarily because it was the largest of the five DOL programs that collected and used SSNs.

The scope of our audit included assessing the procedures DFEC had in place during our fieldwork that were relevant to the disclosure, access, and use of SSN information. We conducted our fieldwork from February to August 2002 at the DOL National Office in Washington, DC.

To perform our audit, we followed the procedures in an audit guide provided by the SSA/OIG for this PCIE initiative. The PCIE SSA/OIG audit guide procedures directed us to confirm the information provided in the CIO's responses to the GAO questionnaires that were relevant to the audit. Following the procedures provided in the PCIE SSA/OIG audit guide, we:

1. interviewed DFEC officials responsible for answering sections of the GAO questionnaire relevant to our audit;

² The questionnaire was part of a study GAO conducted on how and to what extent Federal, state, and local government agencies use SSNs, and how these entities safeguard records or documents containing those SSNs. GAO sent the questionnaires to 14 cabinet-level departments and four agencies.

2. verified and updated relevant information provided on the GAO questionnaire;
3. obtained supporting documentation; and
4. followed up on any vulnerabilities reported in the GAO questionnaire by DFEC officials.

To determine if DFEC had adequate controls over access to SSNs maintained in its databases, we also reviewed and relied on an OIG audit report³ on general controls and security over selected financial management systems, which included the FECA system.

The PCIE SSA/OIG audit guide did not require, nor did our audit include, testing the effectiveness of DFEC controls over the disclosure, access, and use of SSNs.

We also performed work beyond what the PCIE SSA/OIG audit guide required. Specifically, we:

1. Contacted one of the DFEC district offices to obtain documentation and a detailed explanation of the process of disclosing SSNs to physicians responsible for conducting second opinions and independent medical examinations.
2. Visited the DFEC central mail facility that is located in a commercial building in London, Kentucky, and operated by a contractor. Of all OWCP contractors, this one had the most access to SSNs. We obtained a verbal description of the process used to collect and destroy documents that contained SSNs, and we physically observed the controls in place to secure the documents.

We performed our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

³ “U.S. Department of Labor Audit of General Controls and Security for Selected Financial Systems as of September 30, 2001”, OIG Audit Report Number 23-02-002-50-598, issued March 19, 2002

AUDIT RESULTS, FINDINGS, AND RECOMMENDATIONS

Overall, our audit determined that management controls over the disclosure, access, and use of SSNs within the FECA program are generally adequate, but improvements can be made. Following are the results of our audit.

1. Management controls exist to ensure that claimants are informed that their SSNs may be provided to other organizations and that disclosures of SSNs to third parties are legal under the Privacy Act. However, we concluded this process could be improved by revising the standard claimant form to ensure that the FECA claimant has read the Privacy Act Disclosure Statement explaining the use and disclosure of the claimant's SSN prior to signing the form. (See Finding Number 1.)
2. DFEC uses six types of contractors that have access to claimant data including SSNs. We determined that the standard contracts and/or memoranda of understanding used for these contractors contain adequate language pertaining to the Privacy Act and the contractor's responsibility to safeguard the data. However, DFEC monitoring of contractor and other entities' disclosure, access, and use of FECA data is limited to entities under DFEC's direct supervision (e.g., data entry, system management) and large single dwelling contracts (e.g., central mail facility). (See Finding Number 2.)
3. FECA claimant records containing SSNs are provided to physicians who do not have contracts with OWCP. Our review of the process used to provide FECA claimant records to these physicians found that the physicians are not consistently given an adequate explanation of the Privacy Act requirements. Also, we were told there have been incidents where physicians have lost claimant records. (See Finding Number 3.)
4. There are adequate controls over access to DFEC's automated management information system. We found that access is limited to DFEC employees, other Federal agencies, nurses, and record imaging and data entry contractors. There are written agreements with these parties covering the security and use of SSNs. Additionally, we reviewed the report of the most recent OIG audit on the management information system general controls and security, which included DFEC. The report contained one access control finding related to periodic reviews of users' accounts not being conducted on a regular basis, and inactive and revoked user IDs not being removed from the user directory. OWCP was in the process of implementing corrective action.

Our conclusions and recommendations are valid only with regard to the controls that existed during our audit period of February through August 2002. Projection of the adequacy of the DFEC management controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions or deterioration of their effectiveness.

Following are the details of our findings and recommendations.

Finding Number 1. The Standard Claim Forms Need to be Revised.

DFEC needs to revise the standard claim forms so that the claimant's signature is more directly associated with his or her acknowledgement of the Privacy Act Disclosure Statement. The standard claim forms do not focus FECA claimants toward reading the Privacy Act Disclosure Statement, which explains the use and disclosure of their SSNs. This condition exists because the claimant's signature and the Privacy Act Disclosure Statement are found on different pages of the standard claim form, and individuals other than the claimant complete the pages preceding the Privacy Act Disclosure Statement. Having the signature directly associated with the Privacy Act Disclosure Statement will provide better assurance that the claimant, and any other individual responsible for completing the form, is aware that their SSN may be provided to other organizations, and that disclosures of SSNs to third parties are legal under the Privacy Act.

Three types of claims forms are used for Federal workers seeking FECA medical and/or compensation from a work-related injury or illness. The form numbers and titles are:

- CA-1. Federal Notice of Traumatic injury and Claim for Continuation of Pay/Compensation
- CA-2. Notice of Occupational Disease and Claim for Compensation
- CA-5. Claim for Compensation by Widow, Widower, and/or Children

These forms each consist of three or four pages, with the Privacy Act Disclosure Statement appearing on the last page of the document. Federal regulations⁴ require that the person submitting a claim or notice must include the SSN of the injured employee.

Our review of the above forms concluded that while they comply with the Privacy Act requirements, the lay out of the forms does not focus the claimant's attention beyond his/her signature on the first page.

RECOMMENDATION

We recommend that the Assistant Secretary for Employment Standards require OWCP to revise the standard claimant forms to focus the claimant's attention on the Privacy Act Disclosure Statement. This can be accomplished by inserting a line above the first data entries, requiring the claimant (and other respondents) to read the page containing the Privacy Act Disclosure Statement before completing any of the subsequent information.

⁴ 20 C.F.R § 10.100(a)

Auditee's Response

In the response to our draft report, the Assistant Secretary for Employment Standards agreed to revise the standard claimant forms; however, ESA cannot ensure that the claimant is aware of the Privacy Act. Therefore, the Assistant Secretary for Employment Standards requested that we change the wording in the recommendation from “revise the standard claimant forms to ensure that the claimant is aware of the Privacy Act Disclosure Statement” to “revise the standard claimant forms to focus the claimant’s attention on the Privacy Act Disclosure Statement.”

Auditor's Conclusion

We agreed with Assistant Secretary’s response and changed the wording in the recommendation. The recommendation can be resolved when ESA provides the planned dates for achieving the corrective action.

Finding Number 2.**A Cost-Effective Plan for Onsite Monitoring of Contractors and Other Entities Needs to be Implemented.**

DFEC monitoring of contractors' and other entities' use and storage of FECA data is limited to entities under DFEC's direct supervision (e.g., data entry, system management) and large single dwelling contract operations (e.g., central mail facility). We found that DFEC does not conduct any onsite monitoring of its remote site contractors (e.g., nurses, rehabilitation counselors, and physician brokers) or other entities (e.g., second opinion and independent medical exam physicians). DFEC officials told us that, instead of onsite monitoring, they rely on the training they provide to the contractors. However, without adequate onsite monitoring, DFEC cannot ensure that contractors and other entities are complying with security and disclosure requirements.

DLMS 5, Chapter 200, Section 224a, provides the minimum standards for safeguarding personal information from unauthorized or unintentional access, disclosure, modification, or destruction. The DLMS requires personal information be stored in a bar-lock cabinet, safe file, or a room secured by a double-action dead bolt lock. To the extent possible, access to areas where personal records are stored will be limited to those persons whose official duties require them to work in such areas. Control of personal records will be maintained at all times and will include an accounting of their removal from the storage area. This minimum standard is prescribed for non-duty hours as well as for duty hours.

DFEC provides SSN information on FECA claimants to its remote site contractors (e.g., nurses, rehabilitation counselors, and physician brokers) and other entities (e.g., second opinion and independent medical exam physicians) that do not have contracts with OWCP. DFEC does not physically monitor all these contractors and other entities. DFEC officials explained that they do provide training to the contractors as part of their certification process, and the training includes securing and protecting claimant information.

It is our opinion that the training provided to the contractors is not sufficient to ensure that SSNs are properly safeguarded and secured from unauthorized disclosure.

RECOMMENDATION

We recommend that the Assistant Secretary for Employment Standards require OWCP to develop a cost-effective, onsite monitoring program that will provide reasonable assurance that contractors and other entities are complying with the requirements for safeguarding the access and use of FECA claimants' SSNs.

Auditee's Response

In the response to our draft report, the Assistant Secretary for Employment Standards agreed with the recommendation but requested that we specify that the onsite monitoring plan be cost effective.

Auditor's Conclusion

We agreed with Assistant Secretary's response and changed the wording in the recommendation. The recommendation can be resolved when ESA provides the planned dates for achieving the corrective action.

Finding Number 3.
Controls Over the Release of Records to Noncontractor Physicians Need to be Improved.

FECA claimant records containing SSNs are provided to physicians who do not have contracts with DOL. Our review of the process used to provide FECA claimant records to these physicians found: (1) DFEC does not consistently provide these physicians with an adequate explanation of Privacy Act requirements; and (2) there have reportedly been incidents in which physicians have lost FECA claimant records or documents.

According to 5 U.S.C. § 552a section 2, one purpose of the Privacy Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to:

Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that *adequate safeguards are provided to prevent misuse of such information*. [Emphasis added.]

DFEC provides claimant records to two types of physicians who are not under contract with DOL. The first type is physicians who provide second opinions on a claimant's physical or mental status related to the reported injury or illness. These are referred to as second opinion physicians and they are obtained by contracted physician brokers. The second type is physicians who perform independent medical examinations because of disputes arising from diagnosis of the reported injury or illness. These are referred to as IME physicians and they are obtained through a physician national directory.

Privacy Act Notification

Our audit of the process used to provide claimant records to these physicians found that DFEC does not consistently notify the physicians of their responsibilities under the Privacy Act to safeguard the privacy information, such as the SSN. Although DFEC officials believe contracted physician brokers are disclosing claimant records to second opinion physicians in accordance with requirements of the Privacy Act, they could not provide us first-hand knowledge of how the disclosure was being done. Additionally, we found that the cover letter used to disseminate claimant records to IME physicians does not provide an adequate explanation of the Privacy Act requirements.

Claimant Records

We identified a potential problem with the accountability of claimant records provided to IME physicians. When an independent medical examination is needed, it is necessary for the applicable DFEC district office to provide the IME physician the entire claimant case file. The file is needed by IME physicians to assist them in reaching a conclusion on the issue of

the cause and extent of the claimant's impairment. However, we were told by a DFEC district office official that there have been incidents in which IME physicians have lost claimant case files or case files were returned with missing documents.

RECOMMENDATIONS

We recommend that the Assistant Secretary for Employment Standards require OWCP to:

1. Provide second opinion and IME physicians a cover letter when providing them claimant files or documentation, encouraging them to comply with the principles of the Privacy Act.
2. Explore the extent and cause of losses of claimant files or documents by IME physicians and take any necessary corrective action.

Auditee's Response

In the response to our draft report, the Assistant Secretary for Employment Standards agreed with the recommendations. Concerning the incidents of lost claimant files or documents by IME physicians, the Assistant Secretary stated that DFEC has implemented case file imaging, which will eliminate the problem. However, the extent and cause of any lost claimant files by IME physicians will be explored, and any necessary corrective action taken.

Auditor's Conclusion

We agreed with Assistant Secretary's response. The recommendations can be resolved when ESA provides the planned dates for achieving the corrective action.

AGENCY'S RESPONSE TO DRAFT REPORT



DEC 16 2002

MEMORANDUM FOR ELLIOT P. LEWIS

Assistant Inspector General for Audit

D. M. Wilk For

FROM:

VICTORIA A. LIPNIC

SUBJECT:

Audit of Controls Over the Disclosure, Access,
and Use of Social Security Numbers in the
Federal Employees Compensation Act Program
Draft Audit Report Number 03-03-002-04-001

This is in response to your December 3, 2002 memorandum requesting our review and comments on the subject report. ESA has reviewed the report and our comments are attached. If there are questions, Rose Broadwater or Cecily Rayburn may be contacted at 693-0285 or 693-0990, respectively.

Thank you for the opportunity to review and comment on the draft report.

Attachment

**ESA's Response to the OIG Draft Audit Report Entitled
Controls Over the Disclosure, Access, and Use of Social Security Numbers in the
Federal Employees' Compensation Act Program, Report No. 03-03-002-04-001**

The Employment Standards Administration generally agrees with the findings and recommendations in this draft audit report but have the following comments:

Page 5: Number 5, Rehabilitation, in the list of six FECA contractors, incorrectly indicates that DFEC has contracts with numerous vocational rehabilitation counselors. This should read "**OWCP** has contracts. . . ."

Page 7: In the section entitled Scope and Methodology, the first sentence should be corrected to read "We selected **DFEC** for our audit" as opposed to "We selected **FECA** for our audit." In the same section, the draft report incorrectly states that OWCP administers **five** DOL programs: FECA, Black Lung, **Wage and Hour**, Longshore, and Energy Employees' Occupational Illness Compensation. OWCP only administers four programs. OWCP does not administer Wage and Hour.

Page 10: Under the heading Recommendation, we do not believe that we can ever "ensure" that the claimant is aware of the Privacy Act and would prefer to see the following language: We recommend that the Assistant Secretary for Employment Standards require OWCP to revise the standard claimant forms to focus attention on the Privacy Act Disclosure Statement. This can be accomplished. . . ." In addition, the citation to the FECA regulations in footnote four on page 10 should be revised to read "20 C.F.R. § 10.100(a)."

Page 11: In the "Finding Number 2" box at the top of the page, we would like to see the language revised to state: "A **Cost-Effective Plan for Onsite Monitoring of Contractors and Other Entities Needs to be Implemented.**" In the first paragraph, fourth line, we would prefer the wording "**remote site contractors**" as opposed to "**multi-site contractors.**" The same wording substitution should be made in the third paragraph, first line.

Page 12: Under the heading "Privacy Act Notification," second line, the word "**consistently**" should be substituted for the word "**adequately**".

Page 13: In regard to recommendation three, DFEC will provide second opinion and IME physicians a cover letter when providing them claimant files or documentation, explaining in detail the physicians' responsibility to comply with Privacy Act requirements.

Also, DFEC has implemented case file imaging which eliminates loss of claim files. The extent and cause of any loss of claimant files by IME physicians will be explored and any necessary corrective action taken.