UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Safeguarding Social Security Numbers

Report No. OIG-AMR-48-05-05

August 2005

INSPECTOR GENERAL

NATIONAL LABOR RELATIONS BOARD

WASHINGTON, DC 20570

August 31, 2005

I hereby submit an audit on *Safeguarding Social Security Numbers*, Report No. OIG-AMR-48-05-05. This audit was conducted to assess the adequacy of controls at the National Labor Relations Board (NLRB or Agency) over the access to, disclosure of, and use of Social Security Numbers (SSN) by external entities. This audit includes SSNs of Agency employees, vendors, and those collected by program offices for case processing purposes.

The 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. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally impose limitations on how they can be used. The Freedom of Information Act (FOIA) of 1966, the Privacy Act of 1974 (Privacy Act), and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs. Other Federal laws lay out a framework for Federal agencies to follow when they establish information security programs that protect sensitive personal information, such as SSNs. Because the increased use of the SSN as a national identifier provides a motive for unscrupulous individuals to acquire a SSN and use it for illegal purposes, Federal agencies have the responsibility to limit the risk of unauthorized disclosure of SSNs.

The importance of security over SSNs is illustrated by recent events such as a security breach at the Federal Deposit Insurance Corporation (FDIC). On June 18, 2005, CNN reported that the FDIC, which insures many of the nation's banks, alerted 6,000 current and former employees that personal information may have been released and that some individuals could be the victims of identity theft. CNN reported that a letter to FDIC employees said that the breach included names, birth dates, and SSNs. The letter also stated that in a small number of cases the information is known to have been used to obtain fraudulent loans from a credit union.

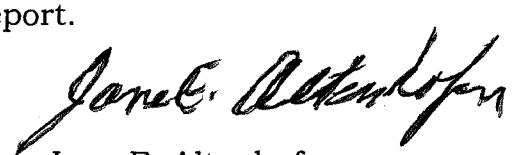
The Agency uses SSNs because its use is required by Federal laws and regulations to identify employees and vendors. Additionally, Regional Offices collect SSNs to help locate parties in unfair labor practice cases and to use in cases in which backpay is a potential remedy.

Generally, the Agency had adequate controls over SSNs in the FOIA process. SSNs were not included in affidavits, which would protect the individual's privacy in judicial proceedings. Three of the four Regional Offices visited adequately secured employee related documents. Also, workday physical inspections of the Regional Offices visited, Security Branch, Office of Employee Development, and Procurement and Facilities Branch did not find any instances of unsafeguarded SSNs. We did observe, however, a few instances at Headquarters in which documents containing personal information, including SSNs, were left in an unsecured manner while the employees in custody were away from their work area.

We determined that improvements were needed to comply with the Privacy Act. The Agency used forms to collect SSNs that did not have the disclosure required by the Privacy Act. One Regional Office did not maintain some personnel records in accordance with Federal regulations or an Agency Privacy Act System of Records notice. The Agency has not published a system of records notice related to Regional Office case files.

We made five recommendations to the Records Management Section Chief, who is also the Agency's Privacy Act Officer. These recommendations were generally to revise forms that do not comply with the Privacy Act requirements regarding the collection of SSNs, inform Regional Offices about the Privacy Act disclosure requirements, update non-NLRB forms provided in the NLRB Web Forms Library, remind employees about maintaining various documents containing SSNs in accordance with Agency policies, and coordinate with Agency management to publish a Privacy Act System of Records Notice for the Case Activity Tracking System and other Regional Office files.

An exit conference was held on July 28, 2005, with representatives of the Division of Administration and the Division of Operations-Management. A draft report was sent to the Records Management Section Chief on July 29, 2005, for review and comment. The Chief's response to the draft report had no comments with respect to the findings, agreed with the recommendations, and indicated planned corrective actions. The response, dated August 30, 2005, is included as an appendix to this report.



Jane E. Altenhofen
Inspector General

TABLE OF CONTENTS

BACKGROUND

The National Labor Relations Board (NLRB or Agency) administers the principal labor relations law of the United States, the National Labor Relations Act (NLRA) of 1935, as amended. The NLRA is generally applied to all enterprises engaged in interstate commerce, including the United States Postal Service, but excluding other governmental entities as well as the railroad and airline industries. The Fiscal Year (FY) 2005 appropriation authorizes 1,865 full-time equivalents that are located at Headquarters, 51 field offices throughout the country, and 3 satellite offices for Administrative Law Judges. NLRB received an appropriation of $251,875,000 for FY 2005, less an across-the-board rescission of .8 percent, leaving a net spending ceiling of $249,860,000.

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. While a number of laws and regulations require the use of SSNs for various Federal programs, they generally impose limitations on how they can be used. The Freedom of Information Act (FOIA) of 1966, the Privacy Act of 1974 (Privacy Act), and the Social Security Act Amendments of 1990 generally govern disclosure and use of SSNs. Other Federal laws lay out a framework for Federal agencies to follow when they establish information security programs that protect sensitive personal information, such as SSNs.

Because the increased use of the SSN as a national identifier provides a motive for unscrupulous individuals to acquire a SSN and use it for illegal purposes, Federal agencies have the responsibility to limit the risk of unauthorized disclosure of SSNs. In 2003, the Social Security Administration (SSA) Office of Inspector General (OIG) coordinated an audit among 15 agencies that are members of the President's Council on Integrity and Efficiency. The SSA OIG reported that most of the reporting agencies had inadequate controls over access to SSNs maintained by the agencies.

The NLRB collects SSNs in many areas of its business. Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, dated November 22, 1943, states that Federal agencies shall use SSNs when identifying individuals. Vendor taxpayer identification numbers, which may include SSNs, are collected in accordance with the Debt Collection Improvement Act of 1996. Additionally, Regional Offices collect SSNs to help locate parties in unfair labor practice cases and to use in cases in which backpay is a potential remedy.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this audit was to assess the adequacy of the Agency's controls over the access to, disclosure of, and use of SSNs by external entities. This audit included SSNs of Agency employees, vendors, and those collected by program offices for case processing purposes. Our scope included transactions involving SSNs at the Agency in calendar year 2004.

We reviewed laws and regulations relevant to safeguarding SSNs, including the Privacy Act and FOIA. We reviewed the Agency's Administrative Policy and Procedures Manual (APPM) to identify procedures for protecting the records of individuals. We reviewed the Agency's Privacy Act Systems of Records Notices to determine our testing universe. We reviewed the NLRB Casehandling Manual and Division of Operations-Management (Operations-Management) memoranda for guidance regarding the handling of SSNs during Agency proceedings.

We interviewed staff in Human Resources Branch (HRB), Security Branch (Security), Procurement and Facilities Branch (PFB), Finance Branch (Finance), Office of Equal Employment Opportunity (OEEO) and the Office of Employee Development (OED) to identify and gain an understanding of controls over SSNs. We evaluated the identified controls. We obtained a list of forms used by the Agency to collect SSNs and determined whether the forms complied with the Privacy Act.

We interviewed employees in the Division of Advice (Advice), Office of Appeals (Appeals), Office of Executive Secretary (OES), and the four Regional Offices visited to learn about how FOIA requests are processed. We selected a statistical sample of 25 FOIA requests in Advice and judgmental samples of 25 FOIA requests in Appeals, OES, and the four Regional Offices visited and determined whether documents containing SSNs were released. The universe of FOIA requests is shown as an attachment to this report.

For each Regional Office visited, we interviewed employees to learn about controls over documents containing SSNs. We evaluated the controls over employee and case processing information. We selected judgmental samples of 25 unfair labor practice cases (C cases) in compliance and 30 C cases in which either a complaint was issued or an unlawful discharge was alleged and tested whether documents that could become public contained SSNs. The universe of these C cases is shown as an attachment to this report.

This audit was performed in accordance with generally accepted government auditing standards during the period of March 2005 through July 2005 at NLRB Headquarters in Washington, D.C. and the following Regional Offices: Region 8 – Cleveland, Region 18 – Minneapolis, Region 20 – San Francisco, and Region 22 – Newark.

FINDINGS

Generally, the Agency had adequate controls over SSNs in the FOIA process. SSNs were not included in affidavits, which would protect the individual's privacy in judicial proceedings. Three of the four Regional Offices visited adequately secured employee related documents. Also, workday physical inspections of the Regional Offices visited, Security, OED, and PFB did not find any instances of unsafeguarded SSNs. We did observe a few instances at Headquarters in which documents containing personal information, including SSNs, were left in an unsecured manner while the employees in custody were away from their work area.

We determined that improvements were needed to comply with the Privacy Act. The Agency used forms to collect SSNs that did not have the disclosure required by the Privacy Act. One Regional Office did not maintain some personnel records in accordance with Federal regulations or an Agency Privacy Act System of Records notice. The Agency has not published a system of records notice related to Regional Office case files.

COLLECTION OF SSNs

Section 7(b) of the Privacy Act states that any Federal, state or local government agency that requests an individual to disclose an SSN shall inform that individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such a number is solicited, and what uses will be made of it. The Government Accountability Office, formerly known as the General Accounting Office, noted in its report *Government Benefits from SSN Use but Could Provide Better Safeguards* that this section applies to all agencies and does not limit the coverage to agencies maintaining a system of records.

NLRB Forms

In the Agency's Web Forms Library on the NLRB Intranet, 178 NLRB forms are listed. Eight forms collect an individual's SSN. As shown in the following table, the eight forms did not completely provide the required information from the Privacy Act, although some forms contained some of the required information or had information that was not specific to providing an SSN.

Disclosures on NLRB Forms Collecting SSNs

NLRB Form	Providing SSN is Mandatory	Authority for Collection	Use of SSN	Complies With Act
NLRB-916 Backpay Claimant Information	No	No	No	No
NLRB-3010 Travel Order	No	No	No	No
NLRB-3065 NLRB Request for Personnel Data	No	No	No	No
NLRB-4180 Authorization to SSA to Furnish Employment and Earnings Information	Yes	No	Yes	No
NLRB-4260 NLRB Annual Travel Order	No	No	No	No
NLRB-4312 NLRB Computation of Backpay	No	No	No	No
NLRB-5411 Employee Assistance Program Lifestyle History	No	No	No	No
NLRB-5493 ACH Vendor / Miscellaneous Payment Enrollment Form	Yes	Yes	No	No

Two of the eight forms, NLRB-916, Backpay Claimant Information and NLRB-4180, Authorization to Social Security Administration to Furnish Employment and Earnings Information, were used to collect information on discriminatees. The NLRB Casehandling Manual states that these forms should be sent to all identified discriminatees when the Regional Office issues a complaint or administratively determines that a charge has merit. Neither the forms nor the correspondence sent by the Regional Offices with the forms included the information regarding SSNs required by the Privacy Act. In addition, Region 18 and Region 22 sent forms developed by the Regional Office to discriminatees that did not contain a Privacy Act Notice about collecting SSNs.

A form not in the Web Forms Library, NLRB-4858, Complaint of Employment Discrimination against the NLRB, is used by OEEO to record the filing of a formal written complaint of employment discrimination against the NLRB. This form contains a Privacy Act Notice, but did not contain information related to the collection of an SSN. Staff in OEEO said that if information relating to SSN collection is required, revisions to the form would be considered.

Non-NLRB Forms

The NLRB Web Forms Library contains 24 forms that are from sources other than the NLRB, 8 of which collect SSNs. Three of the eight forms that collect SSNs do not contain information required by the Privacy Act regarding the collection of SSNs.

- The Standard Form (SF) 182, Request, Authorization, Agreement and Certification of Training, is listed in the Web Forms Library as a single-page document. The hard copy form contains the required notice.

- The Optional Form 612, Optional Application for Federal Employment, is a two-page document in the Web Forms Library. A copy of the form obtained from the Office of Personnel Management (OPM) website contains a third page containing the required information.

- The SF 52, Request for Personnel Action, does not contain the required information. Neither a copy of the form obtained from the OPM website nor the hard copy form contained the required information.

The forms provided in the Web Forms Library were incomplete. These forms are available electronically to provide the user with the convenience of being able to fill out the form electronically.

AFFIDAVITS AND EXHIBITS

OM Memorandum 04-16, *Claimants' Social Security Numbers*, dated December 24, 2003, states that the Regional Offices should ensure that claimants' SSNs are not included on any document that may become public unless required. Documents identified include affidavits, proofs of claim and compliance specifications, as well as any attachments. OM Memorandum 05-57, *Report of FY 2005 Quality Committee*, dated April 20, 2005, noted that SSNs should not be included in an affidavit because of privacy concerns.

SSNs were not included in affidavits in any of the four Regional Offices visited. SSNs were included in exhibits to affidavits in three of the four Regional Offices visited. In Region 18 and Region 20, a significant number of cases had affidavits with exhibits containing SSNs. Documents attached as exhibits to affidavits include pay stubs, employee applications, and lists of employees. The cause of the affidavit exhibits containing SSNs is their submission by the affiant, not the action of the Agency. Operations-Management stated that SSNs could be redacted on the affidavit exhibits if not necessary.

ACCESS TO EMPLOYEE RECORDS

Section 5 CFR 293.106, Safeguarding Information about Individuals, states that personnel records must be stored in metal filing cabinets that are locked when the records are not in use or in a secured room. APPM Chapter REC-2, *Records Management Program*, dated May 12, 2005, states that offices geographically separated from Headquarters may maintain unofficial personnel files, which must be maintained in a secure, confidential manner. In addition, Privacy Act System of Records Notice NLRB-10, Payroll/Personnel Records, states that the records should be maintained behind locked doors.

Employee records were generally maintained in locked filing cabinets in accordance with the regulations in the four Regional Offices visited. Some personnel records in Region 8 were not properly secured. The Region 8 time and attendance records, which contain SSNs, were maintained in an unlocked file cabinet in an unlocked office.

PHYSICAL INSPECTION

Workday physical inspections of the Regional Offices visited, Security, OED, and PFB did not find any instances of unsafeguarded SSNs. The following inadequacies were found in the other offices tested:

- A copy of an SF 50, Notification of Personal Action, was left in the stack of papers to be recycled instead of being placed in a burn bag in HRB. Staff in HRB stated that the document should have been placed in the burn bag and that the employee was informed to do that in the future.

- On two occasions, copies of the NLRB-5493, ACH Vendor/Miscellaneous Payment Enrollment Form, were left unattended on the receptionist's desk in Finance. On one occasion, the document was partially obscured under another paper, but the document was in plain sight on the other occasion. The NLRB-5493 not only contains the Taxpayer Identification Number (either an SSN or an Employer Identification number), but also includes the vendor's banking information. The Finance Branch Chief noted that the employee who occupied the workspace was on vacation and added that forms are left at that desk for action by Finance.

- A stack of SF 182s, Request, Authorization, Agreement and Certification of Training, was left on a desk in Finance while the employee was not at the desk. The items were left with the SSNs in plain sight and accessible to anyone who walked past. The Finance Branch Chief noted that because of the volume of documents containing SSNs that Finance handled, finding forms on an employee's desk is likely at any time.

- A completed Travel Voucher was left on an unattended desk in Operations-Management. The employee's SSN was in plain view. Additionally, completed leave slips were left in plain view in a mailbox in a common area by a door leading to the main hallway. The leave slips have a space for SSNs, but the employee did not place the SSN on the form. Operations-Management noted that a policy for employees not putting the SSN on a leave slip does not exist, but added that such a policy may be considered.

- A folder containing affirmative employment files, which contain SSNs, was left on the credenza of the OEEO employee who maintains the files while the employee was out of the office. Staff in OEEO stated that the records should be maintained in a locked cabinet while the employee was out of the office.

TRAINING FORMS

OED uses the SF 182 for the administration of the Federal Training Program at the Agency. OED stated that the SSN, which is required on the form, is sent to a training provider when the request is used as an authorization document. OED noted that this was not an issue when the multi-copy paper form was used, because the SSN was not provided on the vendor copy of the form.

As a result, SSNs were provided to vendors. In most cases, providing the SSN to the vendor was unnecessary because the vendor only used either the employee's SSN or the last four digits as an identifier on the invoice in 2 of 21 training forms tested. The OED Director stated during our review that a procedure has been implemented to redact the employee's SSN on copies of SF 182s sent to vendors.

PRIVACY ACT SYSTEMS OF RECORD NOTICE

The Privacy Act defines "system of records" as "a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The act further states that each agency that maintains a system of records shall publish a notice in the *Federal Register* establishing the system of records. The act also created criminal penalties for officers or employees of an agency who willfully maintain a system of records without meeting the notice requirements.

The OIG issued OIG-IA-04-01, Top 10 Management Challenges on December 17, 2003, which identified complying with Privacy Act system notice requirements as a serious management challenge. The lack of a Privacy Act system notice was again identified in OIG-IA-05-01, Top Management and Performance Challenges, issued on October 14, 2004.

The Regional Offices visited all maintained files for each discriminatee in compliance cases involving backpay. The files in each Regional Office were maintained by case name, then by the discriminatee name. Because the discriminatee files are retrievable by a personal identifier, they represent a de facto system of records as defined by the Privacy Act. The Agency has not created a System of Records Notice for these records. The Agency had drafted a System of Records Notice NLRB-21, "Case Activity Tracking System and Associated Regional Office Files" in September 2004. The draft System of Records Notice includes files maintained in compliance cases. The System of Records Notice has not been published.

AUDIT FOLLOW-UP

In Inspection Report No. OIG-INS-25-03-03, *Review of Agency Procedures for Control of Identification Badges*, dated March 12, 2003, we noted that the Agency used the last four digits of employees' SSN as an identifier on identification badges (IDs). The Security Branch Chief stated that a new numbering system would be developed and used for new badges beginning March 1, 2003.

Our review of IDs issued subsequent to March 2003 indicated that the last four digits of an employee's SSN are no longer used as the ID number in new IDs. The Security Branch Chief also noted that a standard credential would be implemented for Government employees in the future, and only an employee number would be maintained on the credential.

RECOMMENDATIONS

We recommend that the Records Management Section Chief/Privacy Act Officer:

1. Revise Agency forms that do not comply with the Privacy Act requirements regarding the collection of SSNs.

2. Inform Regional Offices about the Privacy Act requirement to disclose the authority for collecting SSNs, whether providing the SSN is mandatory, and the uses for the SSN.

3. Update non-NLRB forms provided in the NLRB Web Forms Library so that they are complete and current.

4. Remind employees about the importance of maintaining various documents containing SSNs in accordance with Agency policies.

5. Coordinate with Agency management to publish a Privacy Act System of Records Notice for the Case Activity Tracking System and other Regional Office files.

ATTACHMENT

Universe of Transactions Available for Testing

FOIA Requests
Processed in FY 2004

	Cases Processed	Sample Size
Advice	763	25
Appeals	47	25
OES	81	25
Region 8	141	25
Region 18	116	25
Region 20	104	25
Region 22	116	25

Compliance Cases
Calendar Year 2004

	Cases Processed	Sample Size
Region 8	110	25
Region 18	75	25
Region 20	81	25
Region 22	54	25

Complaint Issued or Unlawful Discharge Alleged
Calendar Year 2004

	Cases Processed	Sample Size
Region 8	187	30
Region 18	88	30
Region 20	109	30
Region 22	144	30

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board
Division of Administration
Memorandum

TO: Jane E. Altenhofen
Inspector General

FROM: Tommie Gregg, Sr. 8/30/05
Chief, Records Management Section/Privacy Act Officer

SUBJECT: Comments on Draft Audit Report – "Safeguarding Social Security Numbers " (OIG-AMR-48)

This is in response to your memorandum dated July 29, 2005, in which you requested comments on the draft audit report on the safeguarding of social security numbers. In your memo, you requested that we also indicate our agreement or disagreement with each of the report's findings and recommendations.

We have reviewed the report and have no comments with respect to the findings of the report.

Our comments regarding the report's recommendations are as follows:

1. **Revise Agency forms that do not comply with the Privacy Act requirements regarding collection of SSNs.**

   We agree. We will take appropriate action to ensure that all NLRB forms fully comply with requirements of the Privacy Act.

2. **Inform Regional Offices about the Privacy Act requirement to disclose the authority for collecting SSNs, whether providing the SSN is mandatory, and the uses for the SSN.**

   We agree. We will develop Privacy Act guidance and post it on the Agency's intranet so that all employees are informed about their rights and responsibilities for collecting and safeguarding personal identifiers, such as social security numbers.

3. **Update non-NLRB forms provided in the NLRB Web Forms Library so that they are complete and current.**

   We agree. We have begun adding Privacy Act Statements to relevant non-NLRB forms listed in the NLRB Web Forms Library.

4. **Remind employees about the importance of maintaining various documents containing SSNs in accordance with Agency policies.**

   OM-04-16, dtd December 24, 2003, addresses safeguarding of social security numbers; however, we will develop additional guidance and post it on the Agency's intranet so that all employees are informed about their rights and responsibilities for collecting, maintaining and safeguarding documents containing personal identifiers, such as social security numbers.

5. **Coordinate with Agency management to publish a Privacy Act System of Records Notice for the Case Activity Tracking System and other Regional Office files.**

   We are in the process of finalizing draft Privacy Act System of Records Notice for the Case Activity Tracking System (CATS) and other Regional Office files.

Thank you for the opportunity to comment on the draft report. If you have any questions, please contact me on 273-2833.

cc: The Board
General Counsel
Director of Administration
Associate General Counsel, Operations-Management
Chief, Library and Administrative Services Branch