OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

PROTECTING PERSONALLY IDENTIFIABLE
INFORMATION ON THE
SOCIAL SECURITY ADMINISTRATION'S
INTRANET SITES

August 2009   A-12-09-29118

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- ❑ Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.
- ❑ Promote economy, effectiveness, and efficiency within the agency.
- ❑ Prevent and detect fraud, waste, and abuse in agency programs and operations.
- ❑ Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- ❑ Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.

To ensure objectivity, the IG Act empowers the IG with:

- ❑ Independence to determine what reviews to perform.
- ❑ Access to all information necessary for the reviews.
- ❑ Authority to publish findings and recommendations based on the reviews.

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA)
Intranet sites were protecting personally identifiable information (PII).

BACKGROUND

Office of Management and Budget (OMB) Memorandum M-07-16 requires that
Executive agencies safeguard PII[1] in the Government's possession and prevent its
breach to ensure the Government retains the public's trust. This responsibility is shared
by officials accountable for administering operational, privacy, and security programs;
legal counsel; agencies' Inspectors General and other law enforcement; and public and
legislative affairs offices.[2] It is also a function of applicable laws, such as the *Federal
Information Security Management Act of 2002* and the *Privacy Act of 1974*.[3] OMB
suggested three procedures to reduce the amount of PII available to unauthorized
users:[4]

---

[1] According to OMB M-07-16, PII refers to information which can be used to distinguish or trace an
individual's identity, such as their name, Social Security number (SSN), biometric records, etc. alone, or
when combined with other personal or identifying information which is linked or linkable to a specific
individual, such as date and place of birth, mother's maiden name, etc.

[2] OMB M-07-16, page 1.

[3] Id.

[4] OMB M-07-16, page 2.

- reduce the volume of information collected and retained to the minimum necessary;

- limit access to only those individuals who must have such access; and

- use encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

To meet the OMB requirements, SSA established a PII Executive Steering Committee (ESC) to provide oversight as well as make recommendations on Agency PII policy to the Commissioner. SSA also established other groups to oversee the public Internet site and internal Intranet sites. For example, the Agency established the Web Steering Committee (WESCO) to facilitate coordination between responsible components on the development, management, and maintenance of its public Internet site. In addition, SSA established Internet and Intranet Application Standards Workgroups to oversee the Internet and Intranet sites. By accessing SSA's Internet site, the public can learn about SSA's programs as well as apply for benefits on-line. Access to SSA's Intranet sites is limited to Agency employees. By using SSA's Intranet sites, SSA employees can view information related to SSA's operations, policies, training, etc., through computers connected to SSA's computer networks.[5] The general public cannot view SSA's Intranet sites because they are protected by a firewall.[6]

RESULTS OF REVIEW

Our search of SSA's Intranet sites detected 179 instances of PII being displayed. We found most of this PII on regional Intranet sites maintained by SSA's Office of Disability Adjudication and Review (ODAR). In addition, we found 11 other instances of exposed PII on other SSA Intranet sites containing Agency training manuals. After we notified SSA officials about the exposed PII, it was immediately removed from the Intranet sites. The Agency lacked a designated component to monitor PII issues related to SSA's Internet and Intranet sites. Moreover, SSA had not developed clear and relevant content standards for safeguarding PII on its websites. This lack of controls may have contributed to PII being displayed on SSA's Intranet sites.

PII ON ODAR'S INTRANET SITES

Most of the exposed PII we detected was on ODAR's regional Intranet sites. However, we also found instances of displayed PII on other Agency components' Intranet sites.
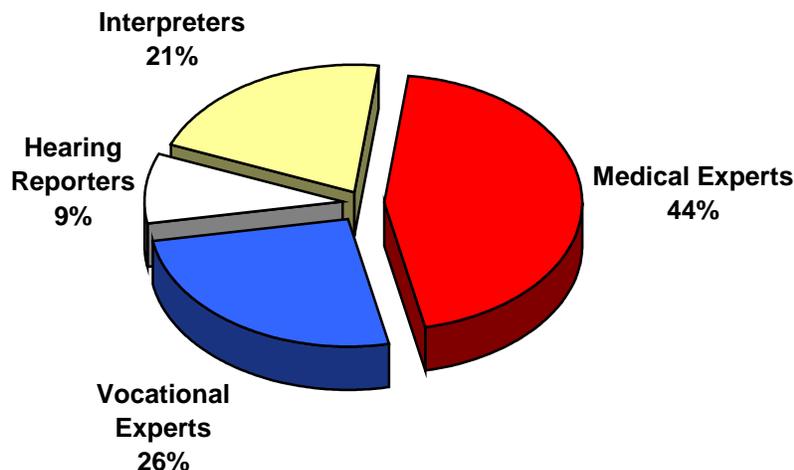
---

[5] Intranet sites can be password-protected to restrict access to a specific group of SSA employees.

[6] A firewall is a software program that acts as a traffic cop and allows only authorized users access to the information. SSA's Central Office administers the firewall software.

PII on SSA Intranet Sites Maintained by ODAR

We found that 2 of ODAR's regional Intranet sites displayed PII on 168 contractors. Using SSA's Intranet search engine, we searched the Intranet sites for PII and found SSNs, Employer Identification Numbers (EIN),[7] personal addresses, and home telephone numbers related to ODAR's contractors (see Figure 1). These contractors include Hearing Reporters, Interpreters, Medical Experts (ME), and Vocational Experts.[8]

Figure 1: PII Displayed on ODAR's Intranet Sites by Contractor Position

Interpreters 21%

Hearing Reporters 9%

Medical Experts 44%

Vocational Experts 26%

In most of the cases, the PII was posted on ODAR regional sites intended to assist other regions in processing hearings. To help manage its growing backlog of pending hearing claims, ODAR was transferring cases between regions. As a result, hearing offices in one part of the country were holding hearings related to claimants in a different part of the country. For instance, an ME at the Bronx Hearing Office in Region II[9] might be required to present evidence at a hearing[10] transferred to the

---

[7] An EIN is a nine-digit number the Internal Revenue Service assigns in the following format: XX-XXXXXXX. According to the Internal Revenue Service, an EIN is also known as a Federal Tax Identification Number and is used to identify a business entity. Only SSNs/EINs with a person's name were included in the number of instances identified where PII was displayed on SSA's Intranet sites, while EINs with an associated business name were not included.

[8] See Appendix C for more information on these contractor positions. Prior SSA Office of the Inspector General audits addressed the internal use of SSA employee SSNs. See *The Social Security Administration's Internal Use of Employee's Social Security Numbers* (A-13-04-24046), issued August 2004, and *Follow-up: The Social Security Administration's Internal Use of Employee's Social Security Numbers* (A-13-07-27164), issued June 2008.

[9] Region II includes New Jersey, New York, and the territory of Puerto Rico.

[10] ODAR has been using video hearings for claims that are transferred from one region to another.

Pittsburgh, Pennsylvania Hearing Office in Region III.[11] To assist the Pittsburgh Hearing Office, the contractor's business information was posted to the Region III's Intranet site.[12] However, in this case, the Intranet site was also displaying sensitive information, such as the ME's SSN, EIN, home address, and telephone number. We found that other ODAR regional Intranet sites were better at protecting this PII by only displaying basic information, such as the contractor's name and a contact telephone number.

After we notified ODAR about the exposed PII, staff immediately removed the sites. Moreover, ODAR staff noted that the Intranet sites in question were no longer being used to assist with workloads.

ODAR Has a More Secure System to Track Contractor PII

ODAR maintains more secure systems to store contractor PII, including the Case Processing and Management System (CPMS)[13] and the Web-Enabled Budget and Administrative Support System (WebBASS).[14] Access to CPMS is based on a user's profile[15] and therefore has tighter controls for accessing contractor PII. SSA uses WebBASS to generate call orders[16] for contractors. Access to WebBASS requires a user name and password.[17]

In addition, ODAR staff stated ODAR's Division of Information Technology Integration (DITI) periodically shares an Excel spreadsheet containing hearing office contractor information with the regional WebBASS points of contact. This spreadsheet assists the hearing offices when cases are transferred within the regions and hearing offices. DITI closely controls this contractor spreadsheet and shares it with ODAR employees on a need-to-know basis.

---

[11] Region III includes Delaware, Maryland, Pennsylvania, Virginia, West Virginia, and the District of Columbia.

[12] The regional sites contained other useful information for the assisting hearing office, such as hearing office contacts, mailing addresses and procedures, hearing calendars, and hotel information.

[13] CPMS is a web-based, user-friendly system that includes interactive screens, a secure and centralized repository of hearing-related data, scheduling capabilities, hyperlinks to reference material, and interfaces with other SSA systems.

[14] SSA uses WebBASS to post and track information about administrative and budgetary items.

[15] A user profile is a collection of personal data associated to a specific user and, as such, contains a digital representation of a person's identity.

[16] A call order is a budget agreement to pay a contractor for its services.

[17] CPMS uses a Contractor Key to interface with WebBASS. The Contractor Key is sent from CPMS to WebBASS where it is matched with the Contractor's name, Blanket Purchase Agreement number and other identifying information.

PII on Other SSA Regional Intranet Sites

We found 11 other instances of PII on other SSA Intranet sites. In addition to SSNs, we found personal addresses, home telephone numbers, and wages displayed on these Intranet sites. The sites were used for posting training manuals to operate SSA's claimant tracking systems. Of the 11 instances,

- 7 contained valid SSNs, but the name did not match SSA's Numident Record,[18] and

- 4 contained valid SSNs with names that matched SSA's Numident Record.

We shared the Intranet links containing PII with SSA's Webmaster, as well as the web managers responsible for creating and maintaining these Intranet sites. We suggested that the web managers replace the valid SSNs with invalid SSNs such as those containing "00" in the group number,[19] since SSA does not issue SSNs with this group number. The web managers either modified or removed the Intranet sites containing the PII.

INTERNAL CONTROLS OVER SSA'S INTERNET AND INTRANET

The Agency lacked a designated component responsible for overseeing PII-related issues on SSA's Internet and Intranet sites. In addition, SSA has not developed clear, relevant content standards for safeguarding PII on its web sites. This lack of oversight may have contributed to PII being displayed on SSA's Intranet sites.

Lack of PII Controls over the Internet and Intranet

In our review of the Internet and Intranet workgroups, as well as discussions with staff in the Office of the Chief Information Officer (OCIO) and Office of Communications (OCOMM), we learned that while SSA has a number of organizations reviewing either PII or the content of the Internet and Intranet sites, no single organization is responsible for preventing PII from being displayed on these sites. For instance, the PII ESC charter does not specifically address the role of the Internet or Intranet sites in disseminating information that could contain PII.[20]

Moreover, WESCO's mission regarding the Internet did not mention the role of the Committee in protecting PII.[21] SSA staff told us that WESCO had coordinated

---

[18] SSA's Numident houses records of original and replacement SSN cards issued over an individual's lifetime, as well as identifying information, such as date of birth, place of birth, and parents' names.

[19] Within each area, the group number (middle two digits) range from 01 to 99 but are not assigned in consecutive order.

[20] See Appendix D for more information on the PII ESC.

[21] See Appendix E for more information on the WESCO.

meetings with SSA's regional Intranet web managers where PII was discussed. However, WESCO relied on the regional Intranet web managers to control PII displayed on regional Intranet sites.

Finally, we found that while SSA's Internet and Intranet Application Standards Workgroups have established standards for displaying information on the Agency's websites, these standards do not discuss controlling the display of PII. The missions of these workgroups relate more to the design of the application rather than its content.[22]

We also found some general content standards for websites on a Web Governance website. The site noted "Sensitive, restricted, or classified information or information that contains PII (such as SSNs) must not be included in any web-based file that could be retrieved using a search engine." However, it appeared this guidance was directed at only the Internet sites, and it was not clear what component, if any, was required to periodically monitor compliance with this provision.

We also spoke to OCIO and OCOMM staff to determine what component had overall responsibility for safeguarding PII at the Agency. OCIO sets Agency policy over PII and is responsible for ensuring OMB mandates are followed, while OCOMM has control and provides guidance over SSA's Internet and Intranet sites. However, neither OCIO nor OCOMM developed content standards for safeguarding PII on SSA's websites, and staff in both offices were unaware of any group charged with this responsibility.

The lack of oversight may have contributed to the PII problems we found on the Intranet sites. Even though the Intranet sites are within SSA's firewall and is not available to the public, the posted information is still available to employees in SSA and can be retrieved using a search engine. Establishing a workgroup with oversight of PII on the Internet and Intranet sites, or adding this to the mission of an existing workgroup, would ensure SSA is following the OMB mandates on the protection of PII.

CONCLUSION AND RECOMMENDATIONS

Our review found PII, including names, SSNs, EINs, home addresses, and wage information, was being displayed on SSA's Intranet sites. Agency Web managers took immediate action to modify or remove the identified Intranet sites. However, while the Agency has a number of groups monitoring PII as well as the Internet and Intranet sites, we could not locate a single organization responsible for preventing PII from being displayed on these sites. This lack of oversight may have contributed to PII being displayed on SSA's Intranet sites.

---

[22] For example, per the Intranet Application Standards Workgroup's website, the Workgroup provides the Agency with a set of Intranet interface design standards for the development of Intranet applications. The Standards provide application developers with a common set of requirements for Webpage, styles, widgets, and controls. The requirements describe how the widget, control, and application should interact with the user in compliance with Agency and Government security policy standards.

To reduce the risk of PII being displayed on SSA's Internet and Intranet sites, we recommend that SSA:

1. Designate a component with the responsibility of (a) developing PII safeguard policies over the Internet and Intranet and (b) ensuring adherence with these new policies.

2. Designate a component with the responsibility of periodically reviewing Internet and Intranet sites to ensure employee and contractor PII is protected. Such reviews should become part of the Agency's internal control structure.

AGENCY COMMENTS

The Agency agreed with our recommendations. See Appendix F for the full text of SSA's comments.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

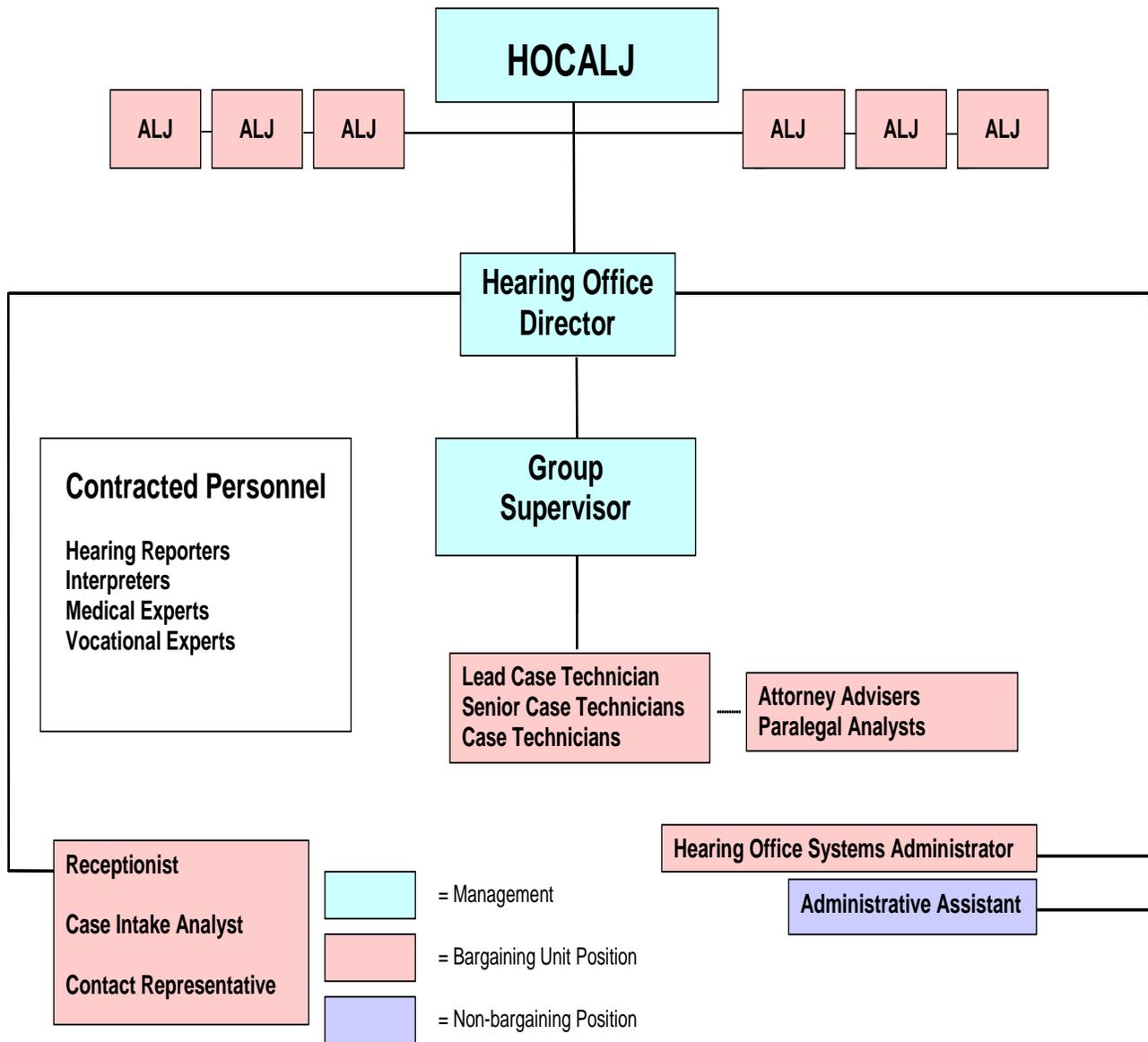|	
ALJ	Administrative Law Judge
COSS	Commissioner of Social Security
CPMS	Case Processing and Management System
DITI	Division of Information Technology Integration
EIN	Employer Identification Number
ESC	Executive Steering Committee
HR	Hearing Reporter
ME	Medical Expert
OCIO	Office of the Chief Information Officer
OCOMM	Office of Communications
ODAR	Office of Disability Adjudication and Review
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SSA	Social Security Administration
SSN	Social Security Number
VE	Vocational Expert
WebBASS	Web-Enabled Budget and Administrative Support System
WESCO	Web Steering Committee

Scope and Methodology

To accomplish our objective, we:

- Reviewed Social Security Administration (SSA) policies and procedures governing the controls over personally identifiable information (PII) as well as employee guidelines established in SSA's *Information Systems Security Handbook*.

- Reviewed Office of Management and Budget Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

- Reviewed prior Office of the Inspector General audits on internal use of Social Security numbers (SSN) and controls over PII.

- Using SSA's Intranet search engine, searched SSA's Intranet sites using the keyword "SSN" to determine whether PII was being displayed on SSA's Intranet sites. Our search revealed over 80,000 Intranet sites with a reference to the keyword "SSN." We examined the first 280 sites for PII.

- Notified SSA's Webmaster, the Office of Disability Adjudication and Review's (ODAR) Webmaster, and Regional web managers about the PII found on their Intranet sites. We shared the Intranet links containing the PII with the Web managers. We verified that the Intranet sites containing PII were either removed or appropriately modified.

- Interviewed ODAR headquarters and regional office staff, SSA's Webmaster, staff at the Offices of the Chief Information Officer and Communications, and a member of SSA's Web Steering Committee.

We performed our review of SSA's Intranet sites from December 2008 through March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Hearing Office Organization Chart and Position Descriptions

Below is an example of a hearing office organization chart for a medium-size hearing office with related position descriptions for contracted personnel who assist the Agency.

```
                           ┌─────────────┐
                           │   HOCALJ    │
                           └─────────────┘
  ┌─────┬─────┬─────┐              │              ┌─────┬─────┬─────┐
  │ ALJ │ ALJ │ ALJ │──────────────┼──────────────│ ALJ │ ALJ │ ALJ │
  └─────┴─────┴─────┘              │              └─────┴─────┴─────┘
                           ┌─────────────┐
                           │Hearing Office│
                           │  Director   │
                           └─────────────┘
```

Contracted Personnel

Hearing Reporters
Interpreters
Medical Experts
Vocational Experts

Group Supervisor

**Lead Case Technician
Senior Case Technicians
Case Technicians**

**Attorney Advisers
Paralegal Analysts**

Hearing Office Systems Administrator

Administrative Assistant

Receptionist

Case Intake Analyst

Contact Representative

☐ = Management

☐ = Bargaining Unit Position

☐ = Non-bargaining Position

Title	Roles and Responsibilities
Hearing Reporters (HR)	The HR's duties are to • be present at the designated hearing site on the date and time specified; • set up and test the digital recording equipment; • record the proper identification information; • monitor the recording equipment to ensure it is functioning properly and a verbatim record of the hearing proceedings is made on the CD during the hearing; • take notes of hearing testimony, ensuring administrative law judge (ALJ) directives pertaining to additional evidence and other needed documents are noted; and • place CD in envelope and place with notes in a designated area in the hearing room after the hearing.
Interpreters	The Social Security Administration provides interpreter services, at no cost, to assist non-English speaking claimants who have difficulty understanding or communicating in English during any part of the hearing process. The interpreter must accurately interpret each word spoken during the hearing for the claimant and, as the claimant answers, listen and render the English version.
Medical Experts (ME)	An ALJ may need to obtain an ME's opinion, either in testimony at a hearing or in responses to written interrogatories, when the • ALJ is determining whether a claimant's impairment(s) meets or equals a listed impairment(s); • ALJ is determining usual dosage and effect of drugs and other forms of therapy; • ALJ is assessing a claimant's failure to follow prescribed treatment; • ALJ is determining the degree of severity of a claimant's mental impairment; • claimant or claimant's representative has requested an ME at the hearing, and the ALJ agrees ME testimony is necessary; • ALJ doubts the adequacy of the medical record in a case and believes an ME may be able to suggest additional relevant evidence; • medical evidence is conflicting or confusing, and the ALJ believes an ME may be able to clarify the evidence;

Title	Roles and Responsibilities
ME (Cont.)	• significance of clinical or laboratory findings in the record is not clear, and the ALJ believes an ME may be able to explain the findings and assist the ALJ in assessing their clinical significance; • ALJ is determining the claimant's residual functional capacity, for example, the ALJ may ask the ME to explain or clarify the claimant's functional limitations and abilities as established by the medical evidence of record; or • ALJ desires expert medical opinion regarding the onset of an impairment. The ALJ must obtain an ME's opinion, either in testimony at a hearing or in responses to written interrogatories, when the Appeals Council or a court so orders. In addition, the ALJ must use an ME to evaluate and interpret background medical test data.
Vocational Experts (VE)	An ALJ may need to obtain a VE's opinion, either in testimony at a hearing or in written responses to interrogatories, when the ALJ is determining whether the • claimant's impairment(s) prevents the performance of past relevant work or • claimant's impairment(s) prevents the performance of any other work and he or she cannot decide the case. The ALJ must obtain a VE's opinion, either in testimony at a hearing or in responses to written interrogatories, when directed by the Appeals Council or a court.

Personally Identifiable Information Executive Steering Committee

In its April 2008 charter, the personally identifiable information (PII) Executive Steering Committee (ESC) states its purpose as follows.

> At the Social Security Administration (SSA), the Commissioner of Social Security (COSS) is the final decision-maker regarding PII loss notification and remediation policy. The COSS is assisted in this task by the PII [ESC], which provides oversight and recommendations on Agency PII policy. The PII ESC also ensures implementation of the Breach Notification Policy and plan.
>
> Stakeholders are the Deputy Commissioners and equivalents of the Agency who are responsible for implementation of Government-required PII protection and security policies. The ESC serves as a forum that supports the COSS by ensuring that all components are aware of evolving PII requirements, SSA policies, and their roles and responsibilities with respect to PII policy implementation.

The core responsibilities of the ESC members include:

- Serving as the principal component contact to the ESC for coordination, implementation, and enforcement of breach-related policies;
- Serving as the principal component contact to the ESC for addressing and reporting PII-specific issues for their component;
- Recommending improvements and updates to Agency breach policies and procedures;
- Developing familiarity with Federal and SSA PII directives, policies, procedures, guidelines, and standards. Keeping up-to-date on policy changes and advising their component and Agency management on current and changing requirements;
- Representing their component's interests to the PII ESC. Ensuring that Federal PII legislation and policies are implemented in their component. Requesting component exceptions to SSA policies and procedures, if exclusion from the standard requirement is warranted;
- Advising Agency management on resources required for implementing breach requirements; and
- Developing and/or coordinating component PII protection and breach programs in conjunction with SSA policies and programs.

Web Steering Committee

The Web Steering Committee (WESCO) was established as the Social Security Administration's (SSA) Internet organization responsible for (1) facilitating coordination between responsible components on the development and management of the Agency's Internet and (2) maintaining the Internet. All components responsible for a presence on the Internet are represented in WESCO. In executing its responsibilities, WESCO is coordinated closely with the Offices of Communications, Operations, and Systems in their respective areas of influence.

- **Policies:** Recommend, interpret, and oversee implementation of the Agency's Web policies.
- **Standards:** Review Agency standards for currency.
- **Procedures:** Establish procedures for the review and approval of SSA's Web products.
- **Enforcement:** Establish enforcement standards for SSA's Web products.
- **New and redesigned sites:** Review new or substantially revised Web products for adherence to technical, usability, accessibility, and editorial standards.
- **Operations:** Provide direction, guidance, and training for Web Managers.
- **Brief SSA executives** on the Agency's Web products and consult with them on overall usage of the Web to achieve their goals.
- **Interagency:** Along with the Chief Information Officer and other appropriate staff, represent and coordinate the Agency's involvement in interagency efforts and other outside efforts that impact the content of SSA's Website.
- **Maintenance:** Coordinate with responsible components the maintenance of their Websites.

Agency Comments

SOCIAL SECURITY

Date: August 7, 2009   Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
          Inspector General

From: Margaret J. Tittel /s/
          Acting Chief of Staff

Subject: Revised Comments on the OIG Draft Report, "Protecting Personally Identifiable Information on
          the Social Security Administration's Intranet Sites" (A-12-09-29118)--INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate OIG's
efforts in conducting this review. Attached is our revised response to the report findings and
recommendations. This response replaces the comments issued on June 24, 2009 and should be
included as part of the final report.

Please let me know if we can be of further assistance. Please direct staff inquiries to
Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "PROTECTING PERSONALLY IDENTIFIABLE INFORMATION ON THE SOCIAL SECURITY ADMINISTRATION'S INTRANET SITES" (A-12-09-29118)

We reviewed the draft report findings and recommendations. We are pleased with the report's acknowledgement that we removed Personally Identifiable Information (PII) from the websites identified in this review. Below please find responses to the specific recommendations.

Recommendation 1

Designate a component with the responsibility of (a) developing PII safeguard policies over the Internet and Intranet and (b) ensuring adherence with these new policies.

Comment

We agree with the intent of the recommendation. We have long-standing policies that govern the protection and disclosure of the information we maintain. These policies apply regardless of how the information is stored (i.e., paper, electronic, or online). Since 2006, the Office of the Chief Information Officer (OCIO) has been responsible for issuing comprehensive agency PII policy, which covers the Internet and Intranet. OCIO published a compilation of all PII policies and recently released a PII Frequently Asked Questions guide. OCIO will work with our components to ensure adherence to our PII policies, including the Internet and Intranet.

Recommendation 2

Designate a component with the responsibility of periodically reviewing Internet and Intranet sites to ensure employee and contractor PII is protected. Such reviews should become part of the agency's internal control structure.

Comment

We agree that periodic reviews of both the Internet and Intranet environments will help ensure no PII resides on those sites. We believe that our current process, whereby the component of jurisdiction is responsible for ensuring that PII is not present on the Internet and Intranet, is a more efficient and effective review. However, given our commitment to protecting the sensitive information we maintain, OCIO will work with the Office of Systems and the Office of Communications to investigate the availability and suitability of automated tools to improve these reviews.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Walter Bayer, Director, Chicago Audit Division

Nicholas Milanek, Audit Manager, Falls Church Office

Acknowledgments

In addition to those named above:

Yaquelin Lara, Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-12-09-29118.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations,
   House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.