OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Needs to Strengthen Its Privacy Program Management Controls

Report No. 2007-P-00035

September 17, 2007

Report Contributors: Rudolph M. Brevard
Charles Dade
Corey Costango

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FOIA	Freedom of Information Act
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information

U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00035
September 17, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine what steps the U.S. Environmental Protection Agency (EPA) took to protect Personally Identifiable Information. We also sought to determine the extent to which EPA put in place a management structure over the Agency's Privacy Program.

Background

Congress passed the Privacy Act of 1974 to protect individual privacy. The Act sets forth requirements for Federal agencies when they collect, maintain, or disseminate information about individuals. Personally Identifiable Information is any information about an individual maintained by an agency – including employment, medical, and financial information – that can be used to trace an individual's identity.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:
www.epa.gov/oig/reports/2007/20070917-2007-P-00035.pdf

EPA Needs to Strengthen Its Privacy Program Management Controls

What We Found

Although EPA has made progress toward establishing its Privacy Program, the program needs more emphasis. EPA needs to set up a more comprehensive management control structure to govern and oversee the program. In particular, EPA needs to establish goals and activities for the Privacy Program and measure progress. Further, EPA needs to update its Privacy Program policies and establish processes to manage and make these policies available to responsible EPA personnel. Also, EPA needs to set up compliance and accountability processes to ensure adherence with key Privacy Program tenets.

These weaknesses existed because of the low priority EPA managers placed on the Privacy Program. A major loss of privacy information could result in substantial harm, embarrassment, and inconvenience to individuals. It could lead to identity theft or other fraudulent use of the information, which in addition to harming the individuals involved could be costly to the Agency and its reputation. Questions on EPA's management of privacy data could also cast doubts over the processes EPA uses to oversee protection of the confidential business information it collects.

What We Recommend

We recommend that the EPA Office of Environmental Information's Director, Office of Information Collection, establish goals and activities for the Agency's Privacy Program. The Director should also establish and use performance measures for the program. Further, the Director should update the Agency's Privacy Program policies and procedures, establish a process for managing compliance, and monitor compliance. We also recommend that this Director work with the Office of Administration and Resources Management to develop sample cascading goals and objectives that EPA managers can use to establish Privacy Program accountability processes. The Agency agreed with the report's findings and recommendations.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

September 17, 2007

MEMORANDUM

SUBJECT: EPA Needs to Strengthen Its Privacy Program Management Controls
Report No. 2007-P-00035

FROM: Patricia H. Hill
Assistant Inspector General for Mission Systems

TO: Mark Luttner
Director, Office of Information Collection
Office of Environmental Information

Kenneth Venuto
Director, Office of Human Resources
Office of Administration and Resources Management

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $135,942.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days. You should include a corrective actions plan for agreed upon actions, including milestone dates. We have no objections to the further release of this report to the public. This report will be available at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact Rudolph M. Brevard, Director for Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Appendices

Purpose

We sought to determine what steps the U.S. Environmental Protection Agency (EPA) took to protect Personally Identifiable Information (PII). We also sought to determine the extent to which EPA put in place a management structure over the Agency's Privacy Program.

Background

Congress passed the Privacy Act of 1974 to protect individual privacy. The Act sets forth the requirements Federal agencies must follow when they collect, maintain, or use information about individuals. The Act requires Federal agencies to respect the privacy of individuals. In this regard, agencies must collect the least amount of information necessary and put in place safeguards to protect the information. Agencies must also allow individuals to inspect their files and correct any erroneous information.

The Office of Management and Budget (OMB) defines PII as any information about an individual maintained by an agency that can be used to distinguish or trace an employee's identity. This includes, but is not limited to, employment, medical, and financial information; social security numbers; date and place of birth; mother's maiden name; and any other personal information that is linked or linkable to an individual.

EPA privacy officials stated that EPA's Office of General Counsel and Office of Administration and Resources Management were responsible for the Privacy Act function prior to Office of Environmental Information (OEI) taking over in 1999. The current EPA privacy policies were established in 1986 and 1987. Further, EPA privacy officials stated that OEI initiated the groundwork for putting in place a Privacy Program by appointing a Privacy Act Officer in 1999. EPA also designated a Senior Agency Official for Privacy, who has overall responsibility and accountability for ensuring the Agency's implementation of information privacy protections, including the Agency's full compliance with Federal laws, regulations, and policies relating to information privacy. OEI tasked its Records, Freedom of Information Act (FOIA), and Privacy Branch with managing the program. The branch is part of the OEI's Office of Information Collection. The branch develops EPA's Privacy Program policies and procedures and oversees implementation of the program.

Noteworthy Achievements

In April 2003, privacy officials indicated OEI launched EPA's first Privacy Act Website and began to raise privacy awareness through training sessions, briefings, and conferences. In June 2006, EPA established a PII workgroup in response to OMB memorandums regarding PII protection. EPA privacy officials also said they established the workgroup to ensure that EPA did everything reasonably possible to protect itself from the accidental or unauthorized release of PII. In addition, the Chief Information Officer (CIO) issued "CIO Policy Transmittal 06-011: Interim Policy and Procedures for Protecting Personally Identifiable Information (PII)," to address PII protection concerns raised by OMB.

Scope and Methodology

We conducted this audit from January through April 2007 at EPA headquarters in Washington, DC, in accordance with generally accepted government auditing standards. To determine steps EPA took to protect PII, we conducted a survey with EPA program and regional offices related to their efforts to put into place processes for protecting PII. Preliminary survey results indicated this area requires further review. After preliminary research, we decided to suspend further work on this objective and to examine this area further during the Fiscal Year 2007 Federal Information Security Management Act audit.

To review the Privacy Program management structure, we interviewed EPA officials responsible for the Agency's Privacy Program. We questioned EPA Privacy Program personnel regarding the following management control areas:

- Policies and procedures
- Roles and responsibilities
- Performance measurement
- Program compliance
- Accountability

We conducted followup interviews, and reviewed relevant documents. Based on information collected during preliminary research, we identified several fundamental weaknesses that require management's immediate attention. Therefore, we decided not to proceed into field work for this objective area and are summarizing our results in this report.

We had not performed prior audits related to the management controls of EPA's Privacy Program. As such, there were no recommendations to follow up on during this audit.

Results of Review

EPA privacy officials stated that EPA is in the process of updating its Privacy Program. However, the Agency needs to put into place a more comprehensive management control structure to govern and support its Privacy Program. In particular, EPA needs to:

- Identify the Privacy Program's key goals and activities, and establish performance measures to assess their progress.
- Update its Privacy Program policies and procedures, and establish processes to manage and make all privacy policies available to EPA personnel.
- Put into place a process to monitor the Privacy Program.

According to Agency officials, these program weaknesses existed because EPA placed a lower priority on the Privacy Program compared to other Office of Information Collection requirements. Activities to strengthen the Privacy Program's internal control structure remain unfinished because of the lack of committed resources or management support. Thus, EPA lacks key processes to proactively manage threats that put the Agency's privacy data at risk. A major

loss of privacy information could result in substantial harm, embarrassment, and inconvenience to individuals. It could lead to identity theft or other fraudulent use of the information, which in addition to harming the individuals involved could be costly to the Agency and its reputation. Questions on EPA's management of privacy data could also cast doubts on the processes EPA uses to oversee protection of the confidential business information it collects.

EPA Needs to Identify Program Goals and Activities and Measure Progress

EPA needs to identify the Privacy Program's key goals and activities, and establish performance measures to assess their progress.

During discussions with EPA privacy officials, the officials identified some informal key goals and activities for establishing and overseeing the EPA Privacy Program. However, these key goals and activities were not identified in any formal policy or strategy document. Without formal key goals and activities to guide the Privacy Program, EPA has no assurance the program will be employed as intended.

In followup correspondence, privacy officials provided a copy of a draft privacy policy, the PII workgroup action plan, and a portion of a Privacy Act program fact sheet. They indicated these documents contained information on key goals of the Privacy Program. While these documents did identify some informal goals and activities, none of the items are recognized in OEI's mission and function manual for the Records, FOIA, and Privacy Branch.

In addition, EPA had not established performance measures for the informal key goals and activities in order to monitor the Privacy Program progress. Without such performance measures, EPA cannot assess the progress of the Privacy Program.

EPA Needs to Update Policy and Establish Change Management and Distribution Processes

EPA needs to update its Privacy Program policies and establish change management and distribution processes for these policies. The current Privacy Program policy is outdated and lacks the specificity needed for duties and responsibilities to be performed uniformly throughout the Agency. EPA privacy officials are currently in the process of drafting a new comprehensive privacy policy and associated procedures and these documents should contain some key components. For example, the new policy and procedures need to provide a consistent means of conducting the work throughout the Agency. Also, the privacy policy and procedures should not only describe who is responsible for what at a high level, but should:

- Clearly describe lower-level assigned responsibilities (i.e., who is responsible, what specifically they are responsible for doing, and how they are expected to do it).
- Establish minimum requirements with which all program/regional offices must comply.

In addition, privacy officials did not have a formal process to manage changes in privacy policies and procedures. It is essential that OEI's Records, FOIA, and Privacy Branch has formal processes in place for managing and ensuring that appropriate changes to its privacy policies and

procedures are made in a timely manner (e.g., updates from OMB, changes in regulations, and changes in roles and responsibilities).

Further, EPA needs to make privacy policies and procedures available to responsible personnel. Agency privacy officials identified two projects that they envisioned would fulfill this role. They plan to establish an intranet site that would provide personnel with access to privacy policies and procedures. Officials also plan to establish a privacy liaison contact within each EPA program and regional office to ensure key documents are distributed. During our review, EPA had not accomplished either of these actions. In a followup response, Agency privacy officials said EPA had delayed development of the intranet site due to issues with funding, personnel, and emerging office priorities. They plan to implement the site in the first quarter of Fiscal Year 2008.

EPA Needs to Establish Compliance and Accountability Processes

EPA needs to establish a monitoring process to ensure that managers and employees are implementing and complying with key tenets of the Privacy Program. Further, the Agency needs to institute a formal process for holding employees and managers accountable for adhering to EPA's policies. EPA's privacy officials indicated they plan to monitor compliance by:

- Establishing responsibilities for Liaison Privacy Officials to perform oversight at the regional and program levels.
- Reviewing Agency forms (both old and new) to ensure the Agency is not collecting unnecessary PII.
- Performing reviews via onsite program visits.

However, EPA has not initiated these activities or formally established a target date for their implementation.

EPA also needs to establish processes to hold employees and managers accountable for adhering to Agency privacy policies. EPA privacy officials said they plan to establish accountability through training, applying incident handling reporting policies, and including a notice to employees of potential sanctions for noncompliance with privacy policy. However, these methods do not establish a process for holding employees and managers accountable for adhering to Agency policies. Normally training is a means to disseminate information rather than hold people accountable. Also, the incident handling policy does not outline a means to hold Agency employees accountable. Further, the notice to employees described only addressed instances when Privacy Act information was actually disclosed to unauthorized personnel. It did not focus on cases where managers and employees are not following Agency policies and procedures intended to limit the risk of disclosure, regardless of whether disclosure actually occurred. Also, these planned methods do not identify processes for linking privacy responsibilities to the performance plans developed under the Agency's Performance Appraisal and Recognition System.

Weaknesses Represent Internal Control Issues

The noted weaknesses are internal control issues within the Privacy Program. According to OMB Circular A-123, "Management's Responsibility for Internal Control," management is responsible for developing and maintaining internal control systems that comply with the following standards:

- *Control Activities:* policies, procedures, and mechanisms in place to help ensure that agency objectives are met.
- *Information and Communication:* information should be communicated to relevant personnel at all levels within an organization. The information should be relevant, reliable, and timely.
- *Monitoring:* periodic assessments should be part of management's continuous monitoring of internal control.

In addition, the "Standards for Internal Control in the Federal Government," issued by the Government Accountability Office in 1999, indicate that control activities include techniques and mechanisms for enforcing management's directives. Internal controls include establishing techniques and mechanisms for holding personnel "accountable" for doing their assigned responsibilities and complying with management directives. In OMB Circular A-130 and OMB Memorandum M-07-16, OMB makes it clear that the agency is required to inform and train managers, supervisors, and employees of their respective responsibilities and the consequences and accountability for violation of these responsibilities. OMB requires agencies to develop and implement appropriate policies outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow rules.

Recommendations

We recommend that the EPA Office of Environmental Information's Director, Office of Information Collection:

1. Establish and formally document key goals and activities for OEI's Records, FOIA, and Privacy Branch associated with EPA's Privacy Program.

2. Establish and track performance measures associated with OEI's Records, FOIA, and Privacy Branch key privacy goals and activities and measure Privacy Program progress.

3. Develop a performance measurement report and share results with the Senior Agency Official for Privacy on at least a quarterly basis. Make performance measurement reports available to EPA offices responsible for implementing the Privacy Program.

4. Update, implement, and communicate EPA's privacy policies and procedures and ensure they adequately address key tenets of the Privacy Program, including clearly communicating:

    a. the minimum requirements with which all program/regional offices must comply.
    b. the roles and responsibilities of all applicable personnel.

c. how the assigned personnel are to specifically perform the work in sufficient detail to ensure the work will be conducted consistently throughout the Agency.
d. the consequences to personnel for not complying with policies and procedures.

5. Identify positions/job types with key Privacy Program responsibilities and develop appropriate sample cascading goals and objectives that EPA managers can use to establish Privacy Program accountability processes within their respective offices. Provide the developed guidance to the Office of Human Resources prior to distributing to Agency personnel for incorporation into the Agency's Performance Appraisal and Recognition System.

6. Develop, maintain, and publish a roster of Agency personnel designated to fill key Privacy Program positions/job types. Make the roster available to EPA personnel.

7. Develop and implement processes for managing EPA privacy policies and procedures to ensure they are updated with appropriate changes.

8. Establish a means of making Agency privacy policies and procedures accessible to EPA personnel.

9. Establish a monitoring and oversight process to help ensure that managers and employees are implementing and complying with the established Agency privacy policies and procedures.

We also recommend that the EPA Office of Administration and Resources Management's Director, Office of Human Resources:

10. Incorporate the guidance developed in response to Recommendation 5 within the Agency's Performance Appraisal and Recognition System and publish the guidance on the Office of Human Resources' Performance Appraisal and Recognition System Website.

Agency Response and OIG Comments

The Director for the Office of Information Collection concurred with our report findings and recommendations. The Director indicated plans are in place to address a number of the recommendations. The Director for the Office of Human Resources indicated the office plans to work with the Office of Information Collection to develop and make available sample cascading goals and objectives that EPA managers can use to establish Privacy Program accountability processes within their respective offices.

Appendix A contains the Director of the Office of Information Collection's August 28, 2007, response to our formal draft report, as well the July 19, 2007, response to our discussion draft report. Appendix B contains the Director of the Office of Human Resources' response to our formal draft report.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	5	Establish and formally document key goals and activities for OEI's Records, FOIA, and Privacy Branch associated with EPA's Privacy Program.	O	Director, Office of Information Collection, Office of Environmental Information			
2	5	Establish and track performance measures associated with OEI's Records, FOIA, and Privacy Branch key privacy goals and activities and measure Privacy Program progress.	O	Director, Office of Information Collection, Office of Environmental Information			
3	5	Develop a performance measurement report and share results with the Senior Agency Official for Privacy on at least a quarterly basis. Make performance measurement reports available to EPA offices responsible for implementing the Privacy Program.	O	Director, Office of Information Collection, Office of Environmental Information			
4	5	Update, implement, and communicate EPA's privacy policies and procedures and ensure they adequately address key tenets of the Privacy Program, including clearly communicating: a. the minimum requirements with which all program/regional offices must comply. b. the roles and responsibilities of all applicable personnel. c. how the assigned personnel are to specifically perform the work in sufficient detail to ensure the work will be conducted consistently throughout the Agency. d. the consequences to personnel for not complying with policies and procedures.	O	Director, Office of Information Collection, Office of Environmental Information			
5	6	Identify positions/job types with key Privacy Program responsibilities and develop appropriate sample cascading goals and objectives that EPA managers can use to establish Privacy Program accountability processes within their respective offices. Provide the developed guidance to the Office of Human Resources prior to distributing to Agency personnel for incorporation into the Agency's Performance Appraisal and Recognition System.	O	Director, Office of Information Collection, Office of Environmental Information			
6	6	Develop, maintain, and publish a roster of Agency personnel designated to fill key Privacy Program positions/job types. Make the roster available to EPA personnel.	O	Director, Office of Information Collection, Office of Environmental Information			
7	6	Develop and implement processes for managing EPA privacy policies and procedures to ensure they are updated with appropriate changes.	O	Director, Office of Information Collection, Office of Environmental Information			

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
8	6	Establish a means of making Agency privacy policies and procedures accessible to EPA personnel.	O	Director, Office of Information Collection, Office of Environmental Information			
9	6	Establish a monitoring and oversight process to help ensure that managers and employees are implementing and complying with the established Agency privacy policies and procedures.	O	Director, Office of Information Collection, Office of Environmental Information			
10	6	Incorporate the guidance developed in response to Recommendation 5 within the Agency's Performance Appraisal and Recognition System and publish the guidance on the Office of Human Resources' Performance Appraisal and Recognition System Website.	O	Director, Office of Human Resources, Office of Administration and Resources Management			

[1] O = recommendation is open with agreed-to corrective actions pending;
C = recommendation is closed with all agreed-to actions completed;
U = recommendation is undecided with resolution efforts in progress

Appendix A

OEI's Office of Information Collection Responses to Draft Report

August 28, 2007

MEMORANDUM

SUBJECT: Response to Draft Audit Report: EPA Needs to Strengthen Its Privacy Program Management Controls Assignment No. 2207-000175

FROM: Mark A. Luttner, Director
Office of Information Collection

TO: Rudolph M. Brevard, Director
Information Resources Management Assessments

As before, I want to thank you for the opportunity to provide comments on the draft audit reporting the findings of your review of EPA's privacy activities (Assignment # 2007-000175). In addition to the comments I submitted to you on July 19th, 2007, which still stand, I would also like to add the following:

1. Along with formally establishing the Agency's National Privacy Program, and communicating roles and responsibilities for all Agency employees, EPA's new Privacy Policy will establish accountabilities and consequences for noncompliance and will integrate privacy and security oversight responsibilities. This new policy will also establish a breach notification response plan to mitigate the risk of harm to individuals if a breach should occur. As stated in my earlier response, this policy is expected to be implemented in the 1st quarter of FY 2008.

2. In conjunction with the comments we have already submitted regarding your recommendation to ***Update Privacy Policy and Establish Change Management and Distribution Processes,*** I would like to underscore that the Privacy Act Intranet Website will also be used as a primary communication tool for the Liaison Privacy Officials (LPO's) network and all Agency employees. The information maintained on this site will be used to keep individuals up-to-date on changes in management, policy and procedures. Among other things, this site will include: the Privacy Program's mission and function statements, milestones with projected completion dates, rules of behavior, the procedures manual for implementation of the Privacy policy, a listing of Privacy Act systems of record due for re-evaluation, a listing of onsite system reviews and dates of their next planned review, PII breaches, and copies of the quarterly privacy reporting under FISMA.

Again, I appreciate the opportunity to provide comments on your draft findings. Please feel free to contact me on 202-566-1628.

July 19, 2007

MEMORANDUM

SUBJECT: Response to Draft Discussion Audit Report: EPA Needs to Strengthen Its Privacy Program Management Controls (Assignment No. 2207-000175)

FROM: Mark A. Luttner
Director, Office of Information Collection

TO: Rudolph M. Brevard
Director, Information Resources Management Assessments
Office of the Inspector General

Thank you for the opportunity to provide comments on the draft discussion report on the findings of your review of EPA's privacy activities. As mentioned in the draft report, EPA is in the process of establishing a more comprehensive privacy program. While there remain areas for improvement, significant strides have been made to protect the personally identifiable information (PII) in the Agency's possession. The Agency is aware of its vulnerabilities and is working to mitigate existing privacy weaknesses with available resources.

EPA is not unlike many other federal agencies rallying to put measures in place to decrease and protect its PII collections in the wake of the Veterans Administration's massive loss of such PII last year. Recognizing its own vulnerabilities, the Agency established a PII Workgroup in June 2006 under the Quality and Information Council (QIC) to identify and implement short- and long-term actions to protect Agency PII from disclosure, including determining the necessity of existing and new PII collection activities. The workgroup developed an action plan with milestones and has completed several critical activities which reduce the Agency's risk to unauthorized access and disclosure of privacy information.

When the responsibility for addressing EPA's privacy activities was transferred to OEI from the Office of General Counsel in 1999, the function primarily consisted of managing the Agency's system of records activities and complying with the 1998 Presidential Order directing agencies to determine if they were in compliance with specific Privacy Act requirements. The Privacy Act Officer, appointed in 2000, managed these largely administrative processes. However, the passage of the E-Government Act of 2002, new FISMA reporting requirements, OMB E-Government scorecards, and growing concerns with identify theft and other privacy-related concerns have expanded the role and responsibilities of the Privacy Act Officer and the need to develop strong internal control structures for protecting privacy information.

EPA's new internal control structures, to a large degree, are set forth in its new Privacy Policy, which we expect to submit to the QIC this quarter. The Policy will bring the necessary direction, guidance and requirements for safeguarding the collection, use, dissemination and storage of PII. The overarching Policy formally establishes the Agency's National Privacy

Program, communicates roles and responsibilities for all Agency employees, establishes accountabilities and penalties, and integrates privacy and security oversight responsibilities. We expect that the policy will begin to be implemented in the 1st Quarter of FY 2008.

I am pleased to report that the Agency made significant progress in the past twelve months addressing many of the weaknesses identified by the OIG in its draft audit report. Many of the actions to address your recommendations are already underway or nearly completed. Specifically, the OIG recommended that the Agency:

- **Create Program Goals and Activities and Measure Progress**.
  The PII Workgroup's Action Plan itemizes the program's key goals and activities. We agree that performance measures for the major activities are needed to assess the progress of the larger program when it is established.

- **Update Privacy Policy and Establish Change Management and Distribution Processes**.
  The Agency is currently updating its privacy policy and procedures. The policy describes responsibilities at a high level and the accompanying procedures describe these responsibilities in more detail and how to perform them. The procedures are being coordinated with the OEI Security Staff. The policy and procedures will be made available to employees on the Agency's Privacy Act Intranet Web site when it is deployed in the 1st Quarter of FY 2008.

- **Establish Compliance and Accountability Process**.
  The Privacy Policy defines the roles and responsibilities of Agency offices, senior officials, managers and employees. It establishes the requirement for offices to designate Liaison Privacy Officials (currently being identified by the programs and regions) to support EPA's management and oversight of its privacy responsibilities. LPOs will provide guidance to their offices and day-to-day oversight with respect to Agency privacy requirements and initiatives. The LPOs will serve as the Privacy Act Officer's support for ensuring that privacy policies, guidance and related information are broadly communicated and will be the points of contact for responding to privacy data calls. The Privacy Act Officer will meet with these individuals on a regular basis. The Privacy Act Officer and OEI Security Staff will work collaboratively to ensure compliance through FISMA reviews and onsite visits. The Privacy Policy will include sanctions for non-compliance.

  The PII Workgroup has nearly completed its review of forms to identify unnecessary PII elements and has met with OARM representatives to better understand the forms management process in order to provide guidance to programs that need to revise forms.

  The PII Action Plan identifies program monitoring as an "ongoing activity". Onsite reviews will begin in the 1st Quarter of FY 2008.

Again, I appreciate the opportunity to provide comments on your draft findings. Please feel free to contact me or Deborah Williams (566-1659) if you have any questions about this memorandum.

cc: Andrew Battin
Sara Hisel-McCoy
Deborah Williams
Judy Hutt
Myra Galbreath
Marian Cody

Appendix B

Office of Administration and Resources Management's Office of Human Resources Response to Draft Report

August 29, 2007

MEMORANDUM

SUBJECT: Comments on EPA's Privacy Program Audit Draft Report

/s/
FROM: Kenneth T. Venuto, Director
Office of Human Resources

TO: Rudolph M. Brevard, Director
Information Resources Management Assessments
Office of the Inspector General

Thank you for the opportunity to comment on EPA's Privacy Program Audit Draft Report. The Office of Human Resources recommends the following substitute language for recommendations #5 and #10 and the "At a Glance" cover page:

Recommendation for #5. "Identify positions/job types with key Privacy Program responsibilities and develop appropriate samples of cascading goals and objectives that EPA managers can use to establish Private Act accountability processes within their respective offices. These samples should be submitted to the Office of Human Resources for review and approval prior to distributing to appropriate senior executives and managers for consideration."

"We recommend that the EPA Office of Administration and Resources Management's Director, Office of Human Resources (OARM/OHR):

Recommendation for #10. "Work with OEI to finalize appropriate sample guidance for managers to use when implementing performance standards for position/job types with key Privacy Program responsibilities. The approved guidance should be posted on OEI's website. For re-enforcement, the link to OEI's website should also be posted on the OHR Performance Appraisal and Recognition System (PARS) intranet website."

Recommendation for "At a Glance" cover page.

In order to make the "At a Glance" cover page consistent with the above recommendations for #5 and #10 of the Draft Report, I recommend the following new language for the last sentence of the "What We Recommend" section:

"We also recommend that the Office of Environmental Information's Director, Office of Information Collection work with the Office of Administration and Resources management's Director, Human Resources, to develop appropriate samples of cascading goals and objectives that EPA managers can use for employees with key Privacy Program responsibilities within their respective office and to establish appropriate methods to communicate these samples."

Again, thank you for the opportunity to comment on EPA's Privacy program Audit Draft Report.

Appendix C

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information
Assistant Administrator for Administration and Resources Management
Director, Office of Information Collection, Office of Environmental Information
Director, Office of Human Resources, Office of Administration and Resources Management
Agency Followup Official (the CFO)
Agency Followup Coordinator
Audit Followup Coordinator, Office of Environmental Information
Audit Followup Coordinator, Office of Administration and Resources Management
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Office of General Counsel
Acting Inspector General