U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

EPA Needs to Improve Safeguards for Personally Identifiable Information

Report No. 14-P-0122 **February 24, 2014**

Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Cheryl Reid
Neven Soliman
Nii-Lantei Lamptey
Rodney T. Allison

Abbreviations

APO	Agency Privacy Officer
DIB	Data Integrity Board
DNP	Do Not Pay
EPA	U.S. Environmental Protection Agency
FY	Fiscal Year
LPO	Liaison Privacy Official
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIC	Office of Information Collection
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information

Cover photo: EPA OIG photo depicting an individual stealing someone else's social security card and driver's license.

Hotline

To report fraud, waste or abuse, contact us through one of the following methods:

email: OIG_Hotline@epa.gov
phone: 1-888-546-8740
fax: 1-202-566-2599
online: http://www.epa.gov/oig/hotline.htm

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW
Mailcode 2431T
Washington, DC 20460

Suggestions for Audits or Evaluations

To make suggestions for audits or evaluations, contact us through one of the following methods:

email: OIG_WEBCOMMENTS@epa.gov
phone: 1-202-566-2391
fax: 1-202-566-2599
online: http://www.epa.gov/oig/contact.html#Full_Info

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW
Mailcode 2431T
Washington, DC 20460

U.S. Environmental Protection Agency
Office of Inspector General

14-P-0122
February 24, 2014

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) must safeguard individuals' Personally Identifiable Information (PII) consistent with the Privacy Act, the E-Government Act of 2002, Office of Management and Budget (OMB) directives, and other federal requirements. Without the proper security controls, the PII is vulnerable to unauthorized access and use.

We sought to determine whether the EPA has developed and implemented policies, procedures and processes for protecting sensitive PII in accordance with federal and agency criteria.

This report addresses the following EPA theme:

- *Embracing EPA as a high performing organization.*

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20140224-14-P-0122.pdf

EPA Needs to Improve Safeguards for Personally Identifiable Information

What We Found

The lack of stronger privacy program processes and procedures places the EPA's sensitive PII at a greater risk of compromise and misuse.

The EPA has not created formal policies and procedures for several processes that contribute to the safeguarding of PII and that ensure compliance with federal requirements. The EPA is using an inaccurate list of systems that contain sensitive PII to report to OMB and the Chief Information Officer. This listing was not up-to-date and it contained incorrect data about systems. Having outdated information may lead OMB and agency management to make decisions that may not be applicable to the agency's needs. The lack of formal policies and procedures and management oversight over agency processes for safeguarding of PII does not ensure employees are aware of their responsibilities for protecting PII.

The PII training process covered 50 percent of the prescribed topics and did not track training of agency personnel. Federal guidance provides specific training topics and directs agencies to train employees on their privacy responsibilities. The agency had not set up a process to track training completion and had not evaluated available privacy training before contracting to develop a new privacy training program. As a result, EPA employees are only trained on a portion of the requirements and management is unable to assess whether all employees have been trained.

Recommendations and Planned Corrective Actions

We recommend that the EPA implement a "rules and consequences" procedure for safeguarding PII; develop policies and procedures for matching programs; develop and implement a process for maintaining an accurate, current listing of systems that contain sensitive PII; implement a process to train individuals who access PII; and conduct reviews of available training before the agency enters into contracts.

The agency concurred with the report's recommendations and provided corrective action plans, which we found acceptable. The agency initially did not agree with recommendation 6 of the draft report and proposed an alternative corrective action. We met with agency officials and revised recommendation 6, and the agency concurred with the revised recommendation.

Noteworthy Achievements

The EPA had created a privacy program as we recommended in a prior Office of Inspector General audit and provided a memorandum to us certifying completion of report recommendations.

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

THE INSPECTOR GENERAL

February 24, 2014

MEMORANDUM

SUBJECT: EPA Needs to Improve Safeguards for Personally Identifiable Information
Report No. 14-P-0122

FROM: Arthur A. Elkins Jr.

TO: Renee Wynn, Acting Assistant Administrator and Chief Information Officer
Office of Environmental Information

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 identified and corrective actions the OIG recommends. The Office of Information Collection is the primary office responsible for the agency program that we reviewed during this audit. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. The agency concurred with all the report's recommendations and provided high-level planned corrective action plans with milestone dates, which we found acceptable.

Action Required

We will close this report upon issuance in our audit tracking system based on your response to the draft report. We believe the proposed actions, when implemented, will adequately address the report's findings and recommendations. Please provide updated information in the EPA's Management Audit Tracking System as you complete each planned corrective action or revise any corrective actions and/or milestone dates. If you are unable to meet your planned milestones, or believe other corrective actions are warranted, please send us a memorandum stating why you are revising the milestones or why you are proposing alternative corrective actions, as required by EPA Manual 2750.

If you or your staff have any questions regarding this report, please contact Richard Eyermann, acting Assistant Inspector General, Office of Audit, at (202) 566-0565 or eyermann.richard@epa.gov; or Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

We sought to determine whether the U.S. Environmental Protection Agency (EPA) has developed and implemented policies, procedures and processes for protecting sensitive personally identifiable information (PII) in accordance with federal and agency criteria.

Background

The Privacy Act of 1974 sets forth requirements for federal agencies when they collect, maintain or disseminate information about individuals. The act requires that federal agencies (a) collect minimal information necessary on individuals, (b) safeguard the information, and (c) allow individuals to inspect and correct erroneous information.

It is the responsibility of the agency to provide information security protection for the use and/or disclosure of information collected or maintained by or on behalf of the agency. It is the policy of the EPA to safeguard individuals' privacy in a manner consistent with the Privacy Act, the E-Government Act of 2002, Office of Management and Budget (OMB) directives and other federal requirements concerning privacy. Without the proper security controls, the PII information collected by agencies is vulnerable to unauthorized access and use.

Responsible Office

The Office of Information Collection within the Office of Environmental Information (OEI) provides oversight of the EPA's National Privacy Program. The EPA National Privacy Program provides leadership, direction and support for the agency's privacy activities by developing policies, procedures, tools and guidance for administering the EPA's requirements under the Privacy Act, the E-Government Act, the Federal Information Security Management Act, and policy and guidance issued by the President and OMB. The Privacy Act officer is the National Privacy Program manager responsible for coordinating and overseeing the agency's Privacy Program, coordinating the publication of a system of records notices with program offices, and providing training or training opportunities for all key privacy personnel and agency employees.

Noteworthy Achievements

The EPA had created a privacy program as we had recommended in a prior EPA Office of Inspector General (OIG) audit and provided a memorandum to OIG certifying completion of report recommendations. The EPA created a privacy policy and an agency-wide privacy program Intranet page.

Scope and Methodology

We conducted this audit 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.

We performed this audit at the EPA headquarters in Washington, D.C., and collected and reviewed information from other EPA locations from December 2012 through August 2013. We reviewed federal requirements and guidelines associated with the safeguarding of PII and compared them to related internal policies and procedures used by the EPA. We also interviewed the EPA privacy officer, system owners and other agency officials to inquire about their internal processes for safeguarding PII.

We randomly sampled six systems that contained sensitive PII, requested system documentation, and reviewed compliance with federal and internal policies and procedures for three of the six sampled systems.

We conducted follow-up on the previous recommendations in an OIG audit report on the EPA's Privacy Program management controls, *EPA Needs to Strengthen its Privacy Program Management Controls,* Report No. 2007-P-00035, dated September 17, 2007. We limited our review to determine whether the EPA took steps to implement the identified recommendations. We did not conduct testing to determine the effectiveness of the recommendations. In this prior report, we recommended that the OEI's Director, Office of Information Collection:

- Establish and formally document key goals and activities for OEI's Records, Freedom of Information Act, and Privacy Branch associated with the EPA's Privacy Program.
- Establish and track performance measures associated with OEI's Records, the Freedom of Information Act, and Privacy Branch key privacy goals and activities and measure Privacy Program progress.
- Update, implement and communicate the EPA's privacy policies and procedures and ensure they adequately address key tenets of the Privacy Program.

- Develop and implement processes for managing the EPA privacy policies and procedures to ensure they are updated with appropriate changes.
- Establish a means of making agency privacy policies and procedures accessible to the EPA personnel.
- 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.

Chapter 2
EPA's Documented Processes for Protecting PII Need Improvement

The EPA's privacy policies and procedures lacked several processes that contribute to the safeguarding of PII and ensure compliance with federal requirements. The OMB and the EPA's Privacy Policy prescribe the practices for implementing the agency's privacy program. These processes were deficient because:

- A formal "rules and consequences" procedure required by OMB Memorandum 07-16 did not exist prior to us questioning the agency.
- Policies and procedures that would govern the need for written agreements in order for the EPA to participate in matching programs with other agencies and would require employees to communicate matching activities to the appropriate officials were not created.
- The EPA did not create oversight processes for ensuring mandated contract reviews were performed to ensure contracts contain language to make the provisions of the Privacy Act of 1974 binding on the contractor and the employees.
- The EPA is using an inaccurate list of systems that contain sensitive PII to report to OMB and the Chief Information Officer on a continuous basis. This listing was not up-to-date and it contained incorrect data about systems. The agency has not developed a process for reviewing and updating this list of systems that contain sensitive PII on a timely basis to ensure accuracy.

Having outdated information, as presented by the listing of systems that contain PII, may lead OMB and agency management to make decisions that may not be applicable to the agency's needs. The lack of formal policies and procedures, and also management oversight over agency processes for protecting PII, does not ensure employees are aware of their responsibilities for protecting PII in accordance with federal requirements. As a result, employees may inadvertently mistreat, misuse and/or expose PII without proper knowledge of their responsibilities.

Formal "Rules and Consequences" Procedure Does Not Exist

The EPA's Privacy Policy contains a high level policy statement addressing "rules and consequences" for protecting PII but needs to publicize specific details via a "rules and consequences" procedure. OMB Memorandum 07-16 states that each agency is responsible for developing and implementing an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions

available for failure to follow these rules. In addition, the memorandum states that policy should describe the terms and conditions that affected individuals shall be subject to and identify available corrective actions.

To comply with the OMB memorandum, the agency developed an Intranet page that contains "rules and consequences." Although this Intranet page contained rules of conduct and consequences with regard to safeguarding PII, the agency had not developed the information on the website into an official agency procedure. Using an Intranet Web page to address a procedure requirement does not ensure that agency personnel are aware of the federal requirements. Employees may inadvertently mistreat, misuse and/or expose PII without proper knowledge of their responsibilities and the consequences for noncompliance.

Agency Lacks Oversight Over a Matching Program

The agency planned to participate in a matching program without providing needed oversight for ensuring that the required documentation exists and appropriate stakeholders are involved. The Privacy Act of 1974 identifies a matching program as any computerized comparison of two or more automated systems of records or a system of records with non-federal records for the purpose of establishing or verifying the eligibility of (or continuing compliance with statutory and regulatory requirements by) applicants for cash or in-kind assistance or payments under federal benefit programs. The Privacy Act of 1974 requires that a source agency and a recipient agency complete a written agreement before disclosing a record from a system of record for use in a computer matching program. The act also requires that the agency's Data Integrity Board (DIB) review, approve and maintain all written agreements for matching programs.

In addition, the EPA's Privacy Policy states that if the agency is involved in a computer matching program, the EPA must establish a DIB, consisting of senior officials, to oversee and coordinate the implementation of the matching program. Lastly, the EPA Privacy Policy states that the agency privacy officer is responsible for oversight over system manager activities to ensure that all privacy-related, statutory and regulatory requirements are met.

The Office of the Chief Financial Officer was preparing to transmit a file from the agency's Compass system into the U.S. Treasury's Do Not Pay (DNP) Portal on March 31, 2013. The Compass financial system replaced the agency's Integrated Financial Management System, which was a System of Record. The agency representatives indicated that the System of Record Notice for the Integrated Financial Management System may still be used for Compass. The EPA never identified the DNP initiative as a likely matching program. In addition, a written matching agreement between the EPA's financial system and the U.S. Treasury's DNP Portal had not been initiated. Also, the agency has not provided coordination or oversight to communicate the need for the DIB to convene in order to oversee

the implementation of this matching program. Lastly, system owners for the data being transferred were not aware of the DIB's role in matching programs.

The EPA has not created written procedures that require a written matching agreement before the agency engages in a matching program that describes how employees are to communicate matching activities to appropriate officials and the privacy office representative. There are also no policies or procedures which require the privacy office representative to solicit responses on a continuous basis from agency regions and program offices to determine the existence of matching programs. As such, the agency representative was not aware that an EPA office was participating in a matching program and the agency representative lacked needed information to advise the DIB to meet to approve agency matching programs. Subsequent to issuing our discussion document, the agency indicated that Office of Technology Solutions representatives indicated that during phase I agency payment files are to be compared against public databases that do not contain PII and, therefore, computer matching requirements are not applicable. However, in phase 2 of the DNP implementation (June 2014 and beyond), the U.S. Department of Treasury will begin using restricted versions of these databases and the EPA would then need matching agreements in place.

Without written procedures, the EPA may not be implementing matching programs in accordance with federal requirements and agency employees may not be able to properly identify and classify ongoing matching program activities. Further, inaccurate information about agency matching programs may be reported to management and OMB.

Mandated Contract Reviews Not Performed

The agency did not conduct required biennial contract reviews. An agency representative stated the contract reviews were last performed in 2008. However, the representative could not provide us with evidence of reviews done since 2008. OMB Circular A-130, Appendix I, requires agencies to review every 2 years a random sample of agency contracts to ensure they contain language to make the provisions of the Privacy Act of 1974 binding on the contractor and the employees. The EPA's *Conducting Privacy On-site Reviews* procedures state that the agency representative will provide instructions to information management officials and Liaison Privacy Officials (LPOs) for conducting Privacy Act reviews as set forth in OMB Circular A-130, Appendix I.

The EPA has not developed an oversight process for ensuring that contract reviews are performed biennially. Also, the EPA's *Conducting Privacy On-site Reviews* procedure does not describe the details for meeting this OMB requirement. By not reviewing a sample of these agency contracts, there is an increased risk that contracts may omit the appropriate language that binds the provisions of the Privacy Act to contractors. As a result, contractors may not be aware that they are responsible for complying with the Privacy Act.

Process for Maintaining PII System List Needs Improvement

The EPA maintains an inaccurate list of systems that contain sensitive PII. OMB Memorandum 07-16 requires agencies to review their current holdings of all PII and ensure, to the maximum extent practical, that such holdings are accurate, relevant, timely and complete. The EPA relies on the program offices to provide information on the agency's systems with sensitive PII. According to the agency, there are no defined intervals as to when program offices are to furnish this to the privacy office, but the process for updating this listing is done on an ad-hoc basis. The agency uses this list of systems to report to OMB and agency management. This report contained inaccuracies.

In our sample of six selected systems that contained sensitive PII, we found that only three were valid systems. The agency is not reviewing and updating the list of systems that contain sensitive PII on a regular basis to ensure accuracy. We concluded that the agency updated the list of sensitive systems only as a result of our audit inquiry. Further, agency policies or procedures do not describe the LPO's responsibilities for updating the Privacy Office on the status of systems with PII. Using an inaccurate list of systems with sensitive PII may lead OMB and agency management to make decisions that may not be applicable to the agency's needs.

Conclusion

The missing elements of the agency's privacy program could significantly degrade the EPA's ability to safeguard PII. Agency employees may not be aware of requirements for safeguarding PII, the EPA could potentially transmit PII without obtaining written agreement, and the agency may have contractors who access PII not informed on responsibilities for complying with privacy requirements. Without additional PII safeguards, the agency may be at risk of PII being mistreated, misused and/or exposed.

Recommendations

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer:

1. Develop an implementing procedure for rules of behavior and consequences.

2. Develop and implement updated agency matching program procedures that:

    a. Define roles and responsibilities for communicating matching activities to the Privacy Office and the DIB.

b. Require a written matching agreement before the agency engages in a matching program.

c. Define the agency Privacy Officer's oversight responsibilities.

d. Convene the DIB for matching programs, as needed.

e. Obtain a written agreement for the current matching program, as needed.

3. Develop and implement an oversight process that describes in detail how the EPA is to perform and document mandated contract reviews.

4. Develop and implement a process for maintaining an accurate, up-to-date listing of systems that contain sensitive PII.

Agency Comments and OIG Evaluation

The agency agreed with these recommendations and provided us with a response to the draft report which included corrective actions with milestone dates. We found the response to be acceptable and updated the report as appropriate. Subsequent to issuing the draft report, we met with the agency to discuss the report's findings and recommendations. As a result of those discussions and the agency's response to the draft, we updated the report as appropriate.

Chapter 3
Privacy Training Not Well Defined or Tracked

The EPA had not annually trained agency personnel on all prescribed topics. The EPA also had not established an oversight process to ensure LPOs and all personnel that access PII are trained. OMB requires agencies to initially train employees on their privacy and security responsibilities before permitting them access to information and information systems. Federal guidance also specifies the topics for training personnel to reduce the possibility that PII will be accessed, used or disclosed inappropriately. The agency incorporates its annual privacy training into the annual information security training but the privacy training portion does not contain all the topics as prescribed by the National Institute of Standards and Technology (NIST). The EPA's process for tracking training lacks steps to ensure that LPOs who miss training obtain training at a later date. Further, the agency's processes lack oversight responsibilities to monitor whether LPOs train their offices' employees. As a result, EPA employees were not trained on all of the prescribed topics for their responsibilities for protecting PII. Senior agency officials may not have the information necessary to take additional measures to address weaknesses in the privacy training program due to the lack of oversight for ensuring personnel are trained.

Privacy Training Topics Not Covered

The EPA had not covered all topics during its annual security awareness training as prescribed by the NIST. OMB memorandum 07-16 requires agencies to initially train employees on their privacy and security responsibilities before permitting them access to information and information systems. It also requires agencies to provide annual refresher training to ensure employees continue to understand their responsibilities. NIST SP 800-122 states that organizations should reduce the possibility that PII will be accessed, used or disclosed inappropriately by training all individuals before being granted access to systems containing PII.

The EPA incorporates privacy training within its annual Information Security Awareness Training. However, this training contains only some of the training topics specified by NIST. As a result, as shown by table 1, the EPA's privacy training program only covers 50 percent of the topics prescribed by NIST.

Table 1: Training topics and EPA training

NIST-specified privacy training topics	Topic included In EPA training
Applicable privacy laws, regulations and policies	N
Restrictions on data collection, storage and use of PII	Y
Roles and responsibilities for using and protecting PII	N
Appropriate disposal of PII	Y
Sanctions for misuse of PII	N
Recognition of a security or privacy incident involving PII	Y
Retention schedules for PII	N
Roles and responsibilities in responding to PII-related incidents and reporting.	Y

Source: NIST topics and OIG analysis.

The agency is developing and updating its privacy training. However, the agency had not evaluated the current privacy awareness training available on its online training portal before it contracted to develop a new training program. When we reviewed the plan progress in July 2013, the training program was approximately 9 percent complete with $9,722 expended. We estimate that the EPA will spend approximately $100,000 to complete development of the new training program.

Without ensuring all privacy training topics are taught, the EPA faces the possibility that agency employees are unaware of all the measures necessary to protect sensitive PII before they are granted access to agency information and information systems.

Privacy Training Not Tracked in Program Offices

The EPA does not have a formal process for tracking the training of agency personnel. The EPA indicated that it has a system in place to track training for their LPOs. In addition, the EPA indicated that the annual security awareness training is tracked centrally, but the EPA has issues with some program offices' training and tracking the training of their staff. We requested verifications from three LPOs regarding the training they provide to their office personnel before they are given access to agency information systems. Two LPOs indicated they did not have training records and appeared to not know the training requirement when they responded that employees did not need training, even though the system in question was identified as containing sensitive PII. One LPO did not respond to our request for information. Our audit also disclosed that the EPA lacks processes to verify whether LPOs responsible for training personnel within their offices monitor the training status of personnel. The EPA's Privacy Policy states that the LPOs are to ensure proper training for individuals in their area of responsibility, including monitoring online training for employees. The policy also designates the agency's Privacy Act Officer with providing oversight to ensure the EPA requirements are met and with training personnel on the policy's privacy requirements.

The EPA offers specialized LPO training once per year and had not set up a process to ensure LPOs that miss the training are trained. While the EPA uses sign-in sheets to track training attendance, the agency neither uses the rosters to identify who missed training nor provides supplemental training to the LPOs to ensure they are kept current about their duties.

Once training is given, it is important to ensure the agency has processes in place to track who completes the training and inform senior agency officials on the status of the training program. The agency lacks necessary internal control processes, including tracking the training status of employees and a mechanism to inform management on the status of their office's training, to ensure the effectiveness of provided training and to make decisions regarding whether additional training is required to ensure employees are aware of their responsibilities necessary to protect PII.

Conclusion

The EPA had not trained all individuals on all prescribed topics for safeguarding PII. Ensuring that agency employees are aware of their responsibilities for protecting PII is critical in order for the agency to ensure it is taking all steps necessary to safeguard PII. Furthermore, the agency does not have an oversight process to track the training of those individuals throughout the agency who have a specialized role in providing privacy training. Without this process, the agency does not have assurance that all individuals are trained in carrying out their duties in support of ensuring that all users who access agency PII know the requirements for safeguarding PII.

Recommendations

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer:

5. Establish and implement a process to train all individuals who access PII based on their roles and responsibilities. This process should include training on all PII topics as prescribed by NIST.

6. Continue with current privacy training plans and establish a process to fully document business cases and due diligence reviews and follow this process should future modifications be needed in the current privacy training contract.

7. Develop and implement an oversight process to monitor that LPOs and all individuals who access PII are trained on their responsibilities for protecting PII. The oversight process should include a method to inform senior agency officials on the status of their office's completion of training.

Agency Comments and OIG Evaluation

The agency agreed with recommendations 5 and 7 and provided high-level corrective action plans with milestone dates which we found acceptable. The agency initially did not agree with recommendation 6. The agency stated the Agency Privacy Officer exercised due diligence by conducting market research before entering into the current contract with the privacy training vendor. However, the agency was not able to provide us evidence to support its assertion. We subsequently met with agency representatives to discuss the finding and related corrective action. Management agreed that steps could be taken to strengthen its oversight processes and we updated the recommendation to be more specific as to the corrective action needed to address the finding. The agency concurred with the updated recommendation and provided us with a high-level corrective action plan with completion dates, which we found acceptable.

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	7	Develop an implementing procedure for rules of behavior and consequences.	O	Assistant Administrator for Environmental Information and Chief Information Officer	9/30/14		
2	7	Develop and implement updated agency matching program procedures that: a. Define roles and responsibilities for communicating matching activities to the Privacy Office and the DIB. b. Require a written matching agreement before the agency engages in a matching program. c. Define the agency Privacy Officer's oversight responsibilities. d. Convene the DIB for matching programs, as needed. e. Obtain a written agreement for the current matching program, as needed.	O	Assistant Administrator for Environmental Information and Chief Information Officer	6/30/14		
3	8	Develop and implement an oversight process that describes in detail how the EPA is to perform and document mandated contract reviews.	O	Assistant Administrator for Environmental Information and Chief Information Officer	3/31/14		
4	8	Develop and implement a process for maintaining an accurate, up-to-date listing of systems that contain sensitive PII.	O	Assistant Administrator for Environmental Information and Chief Information Officer	6/30/14		
5	11	Establish and implement a process to train all individuals who access PII based on their roles and responsibilities. This process should include training on all PII topics as prescribed by NIST.	O	Assistant Administrator for Environmental Information and Chief Information Officer	9/30/14		
6	11	Continue with current privacy training plans and establish a process to fully document business cases and due diligence reviews and follow this process should future modifications be needed in the current privacy training contract.	O	Assistant Administrator for Environmental Information and Chief Information Officer	3/31/14		
7	11	Develop and implement an oversight process to monitor that LPOs and all individuals who access PII are trained on their responsibilities for protecting PII. The oversight process should include a method to inform senior agency officials on the status of their office's completion of training.	O	Assistant Administrator for Environmental Information and Chief Information Officer	9/30/14		

O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is unresolved with resolution efforts in progress

Agency Response to Draft Report

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

NOV '7 2013

OFFICE OF ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY13-0082 *"EPA Needs to Improve Processes for Safeguarding Personally Identifiable Information,"* dated August 19, 2013

FROM:
Acting Assistant Administrator
and Chief Information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations described in the draft audit report.

The Office of Environmental Information's (OEI) response to the audit's findings and recommendations is attached. For the recommendations with which we agree, we provide high-level intended corrective actions and estimated completion dates. For the recommendations with which OEI does not agree, we explain our position and provide proposed alternatives to the recommendations, as appropriate.

EPA's National Privacy Program, established in 2007, is striving to ensure that EPA is in compliance with statutory requirements, guidance and standards issued by the Office of Management and Budget and the National Institute of Standards and Technology. The Program is currently revising the Agency's Privacy Policy to address emerging privacy areas such as social media and cloud computing, and to address privacy needs not identified when the initial policy was issued. The revised Policy is scheduled to be issued in Q2 FY 2014. The Program also is engaged in developing a five-year strategic plan to guide the Agency in meeting its responsibilities to ensure Personally Identifiable Information (PII) is adequately protected.

OEI appreciates this evaluation by the Office of Inspector General (OIG) and the opportunity to address each finding and recommended action. We are committed to ensuring full compliance with federal privacy requirements for protecting Agency PII. If you have questions regarding this response, please contact Judy Hutt, the Agency Privacy Officer, in the Office of Information Collection, Collection Strategies Division, FOIA and Privacy Branch at 202-566-1668.

Attachment

cc: Vaughn Noga
Andrew Battin
Jeff Wells
John Moses
Deborah Williams
Judy Hutt
Scott Dockum
Brenda Young

Attachment 1

Response to OIG Findings and Recommendations

Chapter 2 - EPA's Documented Processes for Protecting PII Need Improvement

OIG Recommendation 1: *Finalize and implement a rules and consequences policy related to safeguarding PII.*

Corrective Action 1: OEI agrees and will develop implementing procedures for rules of behavior and consequences by September 30, 2014. However, we believe we do have a formal rules and consequences policy. (See Agency Privacy Policy, Section 6.)

OIG Recommendation 2: *Develop and implement updated Agency "matching program" policies and procedures.*

Corrective Action 2: OEI agrees that implementing procedures for a matching program are needed and these will be developed. The implementing procedures are planned for completion by June 30, 2014, and will outline the steps required to ensure compliance with the Privacy Act when establishing a matching program. OEI will also include "matching agreements" as a topic in the privacy trainings under development to ensure that key privacy personnel, including managers, are aware of this requirement.

Discussion of OIG Finding 2: Lack of Oversight Over a Matching Program.
OEI believes the report is not accurate in its supporting narrative. The OIG states, "EPA has not created written policies or procedures that require a written matching agreement before the Agency engages in a matching program." EPA's Privacy Policy addresses the matching program requirements for a written matching agreement, along with the requirement to establish a Data Integrity Board (DIB) to oversee any matching activity (see pp. 7, 14 and 15). As we stated previously, the Privacy Act requirements for a matching agreement did not apply to Phase I of the "Do Not Pay" data sharing activity referenced in the report. A matching agreement will be in place to support Phase II of the "Do Not Pay" data sharing activity which will commence in CY 2014.

OIG Recommendation 3: *Develop and implement an oversight process that describes in detail how the EPA is to perform and document mandated contract reviews.*

Corrective Action 3: OEI will develop an oversight process in Q2 of FY 2014 to ensure contract reviews are performed every two years. OEI is currently collaborating with the Office of Administration Resources (OARM) to develop a process for OARM to conduct privacy reviews of contracts and report the results to the Privacy Program. The biennial review process will be documented to guide future reviews.

Discussion of OIG Finding 3: Contract Reviews Not Performed.
The draft report states that OEI could not provide the 010 with either the name of the individual who performed the previous reviews or evidence they were conducted. OEI provided the names of the individuals who performed the contract reviews, along with documentation, but was unable to locate the additional supporting evidence required by the OIG.

OIG Recommendation 4: *Develop and implement a process for maintaining an accurate, up-to-date listing of systems that contain sensitive PII.*

Corrective Action 4: OEI will develop a process for regularly requesting inventory updates from Liaison Privacy Officials (LPOs) and posting the updates to the privacy website. OEI plans to complete this action by June 30, 2014. In addition, OEI will revise its Privacy Policy to describe the LPO's responsibility for reporting on the status of PII systems in their organizations and include this requirement in the privacy training currently being developed for Agency LPOs.

Discussion of OIG Finding 4: Data Used for Official Reporting Not Always U p to Date. OEI disagrees with the statement that an inaccurate listing of systems is used to report to the Chief Information Officer (CIO) and OMB. The Privacy Program regularly updates the list of systems that contain sensitive PII based on information provided by LPOs on the status of these systems. At the time the OIG reviewed the listing of sensitive PII systems posted on the Privacy intranet site, the master list of sensitive PII systems was being reconciled with a recent data call on sensitive PII systems initiated by the Senior Agency Information Security Officer (SAISO).

Chapter 3– Privacy Training Not Well-Defined or Tracked

OIG Recommendation 5: *Establish and implement a process to train all individuals who access Pll based on their roles and responsibilities. This process should include training on all Pll topics as prescribed by NIST.*

Corrective Action 5: The Privacy Program is developing online role-based training courses for key privacy personnel and mandatory general awareness training for all employees, which will be available in Q4 FY 2014. Online trainings for personnel who access PII will cover all PII topics as prescribed by the National Institute of Standards and Technology.

Discussion of OIG Finding 5: Privacy Training Topics Not Covered.
The OIG report states current annual information security training, which has a privacy component, does not cover all the privacy training topics prescribed by the National Institute of Standards and Technology. Privacy trainings conducted by the Agency Privacy Officer, that augment the annual information security training, meet the requirements.

OIG Recommendation 6: *Establish and implement a process to conduct due diligence reviews of available training before the Agency enters into contract s to develop further privacy training.*

Corrective Action 6: OEI disagrees with this finding. The Agency Privacy Officer exercised due diligence by conducting market research before entering into the current contract with the

privacy training vendor. The Agency Privacy Officer was involved in the review and testing of the training identified in the report as "the training on the on line training portal" (i.e., Skillport) and determined the training was not sufficient to meet Privacy Program needs. This evaluation process will continue.

OIG Recommendation 7: *Develop and implement an oversight process to monitor that LPOs and all individuals who access PII are trained on their responsibilities for protecting PI! The oversight process should include a method to inform senior Agency officials on the status of their office 's completion of training.*

Corrective Action 7: Online privacy trainings will be offered and tracked via Skillport, the Agency's online training portal. The Agency Privacy Officer, LPOs and EPA managers will be able to track who has taken the training and provide training opportunities for all who require it. The role-based training for LPOs is scheduled to be available in Q1 FY 2014. The general awareness training is expected to be available later in FY 2014.

Attachment 2

Agency's Response To Report Recommendations

Agreement No.	Recommendation	High-Level lntended Corrective Action(s)	Estimated Completion by Quarter and FY
1	Finalize and implement a rules and consequences policy related to safeguarding PH.	The Agency agrees to develop implementing procedures for rules of behavior and consequences.	4th Quarter FY 2014 (9/30/14)
2	Develop and implement updated Agency matching program policies and procedures that: a. Define roles and responsibilities for communicating matching activities to the APO and the DIB. b. Require a written matching agreement before the Agency engages in a matching program. c. Define the APO's oversight responsibilities. d. Convene the DIB for matching programs, as needed. e. Obtain a written agreement for the current matching program, as needed.	The implementing procedures will outline the steps required to ensure compliance with the Privacy Act when establishing a matching program. The Agency will also include "matching agreements" as a topic in the privacy trainings under development to ensure that key privacy personnel, including managers, are aware of this requirement.	3rd Quarter FY 2014 (6/30/14)
3	Develop and implement an oversight process that describes in detail how the EPA is to perform and document mandated contract reviews.	The Agency will develop an oversight process by March 31, 2014, to ensure contract reviews are performed every two years.	2nd Quarter FY 2014 (3/31/14)
4	Develop and implement a process for maintaining an accurate, up-to-date listing of systems that contain sensitive PII.	The Agency will develop a process for regularly requesting inventory updates from LPOs and posting the updates to the privacy website.	3rd Quarter FY 2014 (6/30/14)

5	Establish and implement a process to train all individuals who access PII based on their roles and responsibilities. This process should include training on all PII topics as prescribed by NIST.	Online trainings for personnel who access PH will cover all PII topics as prescribed by the National Institute of Standards and Technology.	4th Quarter FY 2014 (9/30/14)
7	Develop and implement an oversight process to monitor that LPOs and all individuals who access PII are trained on their responsibilities for protecting PII. The oversight process should include a method to inform senior Agency officials on the status of their office's completion of training.	Online privacy trainings will be offered and tracked via Skillport, the Agency's online training portal.	4th Quarter FY 2014 (9/30/14)

Disagreements

No.	Recommendation	Agency Explanation/Response	Proposed Alternative
6	Establish and implement a process to conduct due diligence reviews of available training before the Agency enters into contracts to develop further privacy training.	The Agency Privacy Officer exercised due diligence by conducting market research before entering into the current contract with the privacy training vendor. The Agency Privacy Officer was involved in the review and testing of the training identified in the report as "the training on the online training portal" (i.e., Skill port) and determined the training was not sufficient to meet Privacy Program needs.	EPA will continue with the current training plans for privacy training in Skillport, the Agency's online training portal.

Attachment 2

Revised Agency Response to Report Recommendations

Agreements

No.	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
1	Finalize and implement a rules and consequences policy related to safeguarding PII.	The Agency agrees to develop implementing procedures for rules of behavior and consequences.	4th Quarter FY 2014 (9/30/14)
2	Develop and implement updated Agency matching program policies and procedures that: a. Define roles and responsibilities for communicating matching activities to the APO and the DIB. b. Require a written matching agreement before the Agency engages in a matching program. c. Define the APO's oversight responsibilities. d. Convene the DIB for matching programs, as needed. e. Obtain a written agreement for the current matching program, as needed.	The implementing procedures will outline the steps required to ensure compliance with the Privacy Act when establishing a matching program. The Agency will also include "matching agreements" as a topic in the privacy trainings under development to ensure that key privacy personnel, including managers, are aware of this requirement.	3rd Quarter FY 2014 (6/30/14)
3	Develop and implement an oversight process that describes in detail how the EPA is to perform and document mandated contract reviews.	The Agency will develop an oversight process by March 31, 2014, to ensure contract reviews are performed every two years.	2nd Quarter FY 2014 (3/31/14)
4	Develop and implement a process for maintaining an accurate, up-to-date listing of systems that contain sensitive PII.	The Agency will develop a process for regularly requesting inventory updates from LPOs and posting the updates to the privacy website.	3rd Quarter FY 2014 (6/30/14)

No.	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
5	Establish and implement a process to train all individuals who access PII based on their roles and responsibilities. This process should include training on all PII topics as prescribed by NIST.	Online trainings for personnel who access PII will cover all PII topics as prescribed by the National Institute of Standards and Technology.	4th Quarter FY 2014 (9/30/14)
6	Continue with current privacy training plans and establish a process to fully document business cases and due diligence reviews and follow this process should future modifications be needed in the current privacy training contract.	The Agency will develop a process to document business cases and due diligence reviews should future trainings be required.	2nd Quarter FY2014 (3/31/14)
7	Develop and implement an oversight process to monitor that LPOs and all individuals who access PII are trained on their responsibilities for protecting PII. The oversight process should include a method to inform senior Agency officials on the status of their office's completion of training.	Online privacy trainings will be offered and tracked via Skillport, the Agency's online training portal.	4th Quarter FY 2014 (9/30/14)

Appendix C

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Education
Principal Deputy Assistant Administrator for Environmental Information
Director, Office of Information Collection, Office of Environmental Information
Deputy Director, Office of Information Collection, Office of Environmental Information
Audit Follow-Up Coordinator, Office Environmental Information