OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Assessing EPA's Efforts to Protect Sensitive Information

Report No. 2006-S-00006

September 19, 2006

Report Contributors: Rudolph M. Brevard
Charles Dade
Cheryl Reid

Abbreviations

CIO	Chief Information Officer
DCI	Data Collection Instrument
ECIE	Executive Council on Integrity and Efficiency
EPA	U.S. Environmental Protection Agency
FAEC	Federal Audit Executive Council
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PAS	Privacy Act Statement
PCIE	President's Council on Integrity and Efficiency
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
SP	Special Publication
VPN	Virtual Private Network

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

OFFICE OF
INSPECTOR GENERAL

September 19, 2006

MEMORANDUM

SUBJECT: Assessing EPA's Efforts to Protect Sensitive Information
Report No. 2006-S-00006

TO: Charles Coe
President's Council on Integrity and Efficiency

Attached is the U.S. Environmental Protection Agency Office of Inspector General's completed Data Collection Instrument, as prescribed by the President's Council on Integrity and Efficiency (PCIE) to use in meeting its requirements under Office of Management and Budget (OMB) Memorandum M-06-16, Protection of Sensitive Agency Information.

In accordance with the PCIE Federal Audit Executive Council reporting instructions, I am forwarding this report to you for consolidation with other Federal Agency OIG reports, and subsequent submission to the Director, OMB. Should you have any questions regarding this report, please contact Rudolph Brevard at (202) 566-0893 or brevard.rudy@epa.gov, or Cheryl Reid at (919) 541-2256 or reid.cheryl@epa.gov.

Sincerely,

Bill A. Roderick
Acting Inspector General

APPENDIX I: IG DATA COLLECTION INSTRUMENT

This data collection instrument (DCI) was developed by the Federal Audit Executive Council (FAEC) Information Technology (IT) Committee of the President's Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency (ECIE) to assist Inspectors General (IGs) in determining their Agency's compliance with Office of Management and Budget (OMB) Memorandum M-06-16. The data collection instrument contains three parts. The first part is based on a security checklist developed by the National Institute of Standards and Technology (NIST) (see Section 1 below). Questions in the DCI are designed to assess Agency requirements in the memorandum, which are linked to NIST Special Publication (SP) 800-53 and 800-53A. Each IG can use the associated checklist and the relevant validation techniques for their own unique operating environment. Section 2 is the additional actions required by OMB M-06-16. Section 3 should document your overall conclusion as well as detailed information regarding the type of work completed and the scope of work performed.

For each overall Step and Action Item, please respond **yes, no, partial, or not applicable**. For no, partial, and not applicable responses, please provide additional information in the comments sections. After the yes, no, partial, or not applicable response, IGs have the option to provide an overall response using the six control levels as defined below for the overall Step. Each condition for the lower level must be met to achieve a higher level of compliance and effectiveness. For example, for the control level to be defined as "Implemented", the Agency must also have policies and procedures in place. The determination of the control level for each Step should be based on the responses provided to the Action Items included in that Step.

Controls Not Yet in Place - The answer would be "Controls Not Yet in Place" if the Agency does not yet have documented policy for protecting personally identifiable information (PII).

Policy - The answer would be "Policy" if controls have been documented in Agency policy**.**

Procedures - The answer would be "Procedures" if controls have been documented in Agency procedures**.**

Implemented - The answer would be "Implemented" if the implementation of controls has been verified by examining procedures and related documentation and interviewing personnel to determine that procedures are implemented**.**

Monitor & Tested - The answer would be "Monitor & Tested" if documents have been examined and interviews conducted to verify that policies and procedures for the question are implemented and operating as intended.

Integrated - The answer would be "Integrated" if policies, procedures, implementation, and testing are continually monitored and improvements are made as a normal part of Agency business processes.

APPENDIX I: IG DATA COLLECTION INSTRUMENT

PLEASE PROVIDE YOUR RESPONSES USING THE DROP DOWN MENU IN GRAY

Section One

Security Controls and Assessment Procedures

Security Checklist For Personally Identifiable Information That Is To Be Transported

and/ or Stored Offsite, Or That Is To Be Accessed Remotely	**REQUIRED RESPONSE**	**OPTIONAL RESPONSE**
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitor & Tested***
		Integrated
STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?	*Partial*	
Action Item 1.1: Has the Agency verified information categorization to ensure identification of personal identifiable information requiring protection when accessed remotely or physically removed?	*Partial*	
Comments: Agency representatives stated during Phase I of the Personally Identifiable Information (PII) Workgroup's Action Plan they reviewed 43 existing Systems of Records Notices to determine: 1) if the collection is still necessary, 2) if all the PII elements are required, 3) if there are elements being collected unnecessarily that can be removed, and 4) if the routine uses are still relevant. The Agency has not yet identified all PII; this is listed as a planned tasks during Phase II in the Workgroup's Action Plan.		
Action Item 1.2: Has the Agency verified existing risk assessments?	*No*	
Comments: The Agency has not yet established a baseline of all Agency systems that contain PII.		
OVERALL STEP 1 COMMENTS: The Agency has not yet identified all PII.		

	REQUIRED RESPONSE	**OPTIONAL RESPONSE**
	Yes	***Controls Not Yet in Place***
	No	***Policy***
Procedure	***Partial***	***Procedures***
	Not Applicable	
STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?	*Partial*	
Action Item 2.1: Has the Agency identified existing organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	*Yes*	
Comments: The Agency implemented an interim Policy for Protecting PII. The policy addresses implementing specific safeguards for protecting PII that is accessed remotely or physically removed.		

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Action Item 2.2: Does the existing Agency organizational policy address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?	*Partial*	
	Yes	
1. For personally identifiable information physically removed:	*Partial*	
a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?		
b. For personally identifiable information that can be removed, does the policy require that information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protection provided by the encryption?	*Yes*	
2. For personally identifiable information accessed remotely:		
a. Does the policy explicitly identify the rules for determining whether remote access is allowed?	*No*	
b. When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using Agency-issued authentication certificate(s) or hardware tokens?	*Yes*	
c. When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.)		
Comments: The Agency implemented an interim Policy for PII. This policy addresses specific safeguards for protecting PII that is accessed remotely or physically removed by employees. However, this interim policy does not include requirements for ensuring that: 1) appropriate training and accountability measures are in place, and 2) a VPN connection established using Agency-issued authentication certificate(s) or hardware tokens is used for remote access of PII. In addition, the policy does not address encryption requirements for transporting and/or remotely storing backup media that contain PII.		
Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?	*Partial*	
Comments: All PII data in electronic format taken offsite by an employee must be encrypted. The Agency has not yet identified all instances where PII is being transported to and stored at remote sites.		
OVERALL STEP 2 COMMENTS: The Chief Information Officer's (CIO's) interim policy does not include specific requirements for: 1) training and accountability measures, 2) using a VPN connection established using Agency-issued authentication certificate(s) or hardware tokens for all remote access of PII, and 3) encrypting backup media containing PII that is transported and/or stored offsite.		

APPENDIX I: IG DATA COLLECTION INSTRUMENT

		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitor & Tested***
		Integrated
STEP 3: Has the Agency implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level?	*Partial*	
Action Item 3.1: In the instance where personally identifiable information is transported to a remote site, have the NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form been implemented?	*Partial*	
Comments: The CIO's interim policy states that all PII data in electronic format taken offsite by an employee must be encrypted. All encryption technologies used to transport and work on PII offsite must be validated according to the Federal Information Planning Standards 140-2. The Agency has not yet identified all instances when backup media that contain PII is being transported to remote sites and whether transportation methods use encryption.		
** Evaluation could include an assessment of tools used to transport PII for use of encryption.*		
Action Item 3.2: In the instance where PII is being stored at a remote site, have the NIST SP 800-53 security controls ensuring that information is stored only in encrypted form been implemented?	*No*	
Comments: The Agency has not yet identified all instances when backup media that contain PII is being stored at remote sites and whether storage methods use encryption.		
** Evaluation could include a review of remote site facilities and operations.*		
OVERALL STEP 3 COMMENTS: The Agency has not yet identified all instances where PII is being transported and/or stored offsite.		
If personally identifiable information is to be transported and/or stored offsite		
follow Action Item 4.3, otherwise follow Action Item 4.4		

APPENDIX I: IG DATA COLLECTION INSTRUMENT

	REQUIRED RESPONSE	OPTIONAL RESPONSE
		Controls Not Yet in Place
	Yes	***Policy***
	No	***Procedures***
Procedure	***Partial***	***Implemented***
	Not Applicable	***Monitor & Tested***
		Integrated
STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?	*No*	
Action Item 4.1: Have NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection been implemented by the Agency?	*No*	
Comments: The Agency has several remote access methods. One method has a VPN and is used mainly by external business partners (nonemployees) to access EPA networks. However, the CIO's interim policy directs employees to use two specific remote access methods, neither of which include the VPN remote access method.		
** Evaluation could include a review of the configuration of VPN application(s).*		
Action Item 4.2: Have the NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information been enforced by the Agency?	*No*	
Comments: The Agency has not identified all PII. In addition, the interim Agency policy does not include all NIST SP 800-53 security controls. For example, the policy does not include NIST SP 800-53 AC- 4 "Information Flow Enforcement" Control. This control requires that the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		
** Evaluation could include a review of controls for downloading PII.*		
If remote storage of personally identifiable information is to be permitted follow		
Action Item 4.3, otherwise follow Action Item 4.4.		
Action Item 4.3: Have the NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information been implemented by the Agency?		
	No	
Comments: The Agency has not yet identified all instances of remotely stored PII. The Agency has not enforced that all remotely stored PII be encrypted.		
Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?	*Not Applicable*	
Comments:		
OVERALL STEP 4 COMMENTS: The Agency has several remote access methods. One method has a VPN and is used mainly by external business partners (nonemployees) to access EPA networks. However, the policy does not require the use of a VPN to remotely access PII. In addition, Agency policy does not address all controls specified in SP NIST 800-53. Furthermore, the Agency has not yet identified all PII that is remotely transported and/or stored or enforced encryption of this PII.		
(The source for all the control steps above is NIST SP 800-53 and SP 800-53A assessment procedures.)		

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Section Two	
Additional Agency Actions Required by OMB M-06-16	
	Yes
	No
Procedure	***Partial***
	Not Applicable
1. Has the Agency encrypted all data on mobile computers/devices which carry Agency data unless the data is determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?	*No*
Comments: The Agency does not encrypt all data on mobile computers/devices unless the data is determined to be non-sensitive, in writing by the Deputy Administrator or designee. Instead, the CIO's interim policy requires Senior Information Officials (SIOs) to approve, in writing, employees who work on PII at offsite locations and that this PII must be encrypted. Employees are prohibited from downloading and/or locally storing PII unless specifically authorized in writing by the SIO. If authorized by the SIO to download and/or locally store PII, employees must save PII files in an encrypted form. SIO's must establish procedures to document all approved downloads and/or local storage of PII and document proper encryption.	
2. Does the Agency use remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access?	*Partial*
Comments: EPA's Remote Access Website identifies several forms of remote access. Two of the methods are described on the website as (1) having two-factor authentication and (2) encrypting the entire remote access session.	
3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?	*Partial*
Comments: The Agency has several remote access methods. The Agency policy requires time-out settings of 30 minutes for two of the remote access methods. The Agency's Chief Technology Officer has issued a memorandum requiring Information Resource Management Branch Chiefs, Information Security Officers, and Information Management Officers to help employees implement setting of Blackberry devices to time-out at 30 minutes or less. If employees utilize a PDA other than a Blackberry, they must follow these same practices and enable their device's password protection capabilities.	
4. Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data has been erased within 90 days or its use is still required?	
Comments: The CIO issued an interim policy on August 23, 2006. It requires all SIOs throughout the Agency to approve, in writing, employees who work on PII at offsite locations by using a mandatory approval form included in this policy. Each SIO must establish procedures to document all approved downloads and/or local storage of PII. Each SIO must also ensure that all such PII has been erased within 90 days using the tools and procedures appropriate to individual file deletion, according to the EPA Procedures for Disk Sanitization, or verify and authorize its continued use. Due to the short time interval between the date the policy was issued and our reporting deadline, we were unable to verify whether these procedures were established and implemented throughout the Agency. We plan to audit EPA's PII controls in FY 2007.	

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Section Three

To assist the PCIE/ECIE in evaluating the results provided by individual IGs and in creating the government-wide response, please provide the following information:

Type of work completed (i.e., assessment, evaluation, review, inspection, or audit).

OIG Response: Assessment - Due to the time constraints, the scope of our work involved focused interviews and examinations of documents. We plan to audit EPA's PII controls in FY 2007.

Scope and methodology of work completed based on the PCIE/ECIE review guide Step 2 page 4. ***(Please address the coverage of your assessment, and include any comments you deem pertinent to placing your results in the proper context.)***

OIG Response: We conducted focused interviews with EPA's Security and Privacy Offices. We performed focused examinations of the 1) CIO's Interim Policy and Procedures for Protecting Personally Identifiable Information, 2) Office of Environmental Information Website describing remote access methods, 3) PII Workgroup Action Plan, 4) list of Systems of Records Notices, and 5) Agency memorandum on configuring Blackberry and PDA devices.

Assessment Methodologies Used to Complete the DCI Sections

	Mark All That Apply				
	Section One				Section Two
	Step 1	Step 2	Step 3	Step 4	
Interviews (G/F/C)	**F**		**F**	**F**	
Examinations (G/F/C)	**F**	**F**	**F**	**F**	**F**
Tests (independently verified - Y/N)	**N**	**N**	**N**	**N**	**N**

Assessment Method Descriptions consistent with NIST SP 800-53A - Appendix D pages 34 - 36.

G *= Generalized.* ***F*** *= Focused.* ***C*** *= Comprehensive.* ***Y*** *= Yes.* ***N*** *= No.*

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Overall Summary Statement. (Please refer to page five of the review guide for sample language for summary statements.)

Based on our assessment, we found that the Agency has taken the following steps to protect its sensitive personal information:

Created a PII Workgroup and three phase Action Plan.

- − During Phase I the workgroup reviewed the Agency's existing Systems of Records Notices to determine: (1) if the collection is still necessary, (2) if all the PII elements are required, (3) if there are PII elements being collected unnecessarily and can be removed, and (4) if the routine uses (i.e., disclosures to other parties) are still relevant.

− During Phase II the workgroup plans to: 1) establish Agency baseline of systems that contain PII by identifying all Agency systems that require Privacy Impact Assessments and determining if additional Systems of Records Notices are needed, 2) review Agency forms to determine if PII is collected; if any/all PII elements on the form are needed; ensure Privacy Act Statement (PAS) is present on form collecting PII and whether the PAS is adequate, 3) review final draft Privacy Policy to ensure PII concerns are adequately addressed and 4) determine the procedures required to fully implement the Privacy Policy.

− During Phase III the workgroup plans to: 1) identify critical training needs, 2) coordinate Security and Privacy Oversight Responsibilities/Activities, 3) address privacy in Agency contracts, and 4) submit report to the Administrator.

Issued CIO Policy Transmittal 06-011: Interim Policy and Procedures for Protecting Personally Identifiable Information (PII).

- Updated the Standard Configuration Document for Blackberry Devices to Safeguard Information.
-

The Agency needs to improve in the following areas:

Identify all PII information.

- Ensure the policy includes specific requirements for 1) training and accountability measures, 2) using a VPN connection established using Agency-issued authentication certificate(s) or hardware tokens for all remote access of PII, and 3) encrypting PII that is transported and/or stored offsite.

Distribution

Office of the Administrator
Agency Followup Official
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Acting Inspector General