DOE F 1325.8
(08-93)
United States Government

Department of Energy

Memorandum

DATE: September 20, 2006 Audit Report Number: OAS-L-06-20

REPLY TO ATTN OF: IG-34 (A06TG036)

SUBJECT: Special Report on "The Department's Security over Personally Identifiable Information"

TO: Chief Financial Officer, CF-1
Chief Human Capital Officer, HR-1
Chief Information Officer, IM-1

INTRODUCTION AND OBJECTIVE

The Department of Energy (Department) maintains numerous information systems that contain personally identifiable information (PII). In response to recent security incidents involving the loss or compromise of sensitive personal information by Federal agencies, the Office of Management and Budget (OMB) issued a memorandum on June 23, 2006, recommending that agencies take action to strengthen controls over the protection of PII within 45 days. The actions focused on ensuring that PII was adequately protected when transported or remotely accessed. The guidance also recommended that all computer-readable extracts from databases containing sensitive data be tracked and promptly erased when no longer needed.

In response to a request from OMB, the Office of Inspector General (OIG), in coordination with the President's Council on Integrity and Efficiency (PCIE), performed a review of the Department's controls over the protection of PII. The review was based on a PCIE developed standardized guide designed to test the implementation of OMB guidance and related National Institute of Standards and Technology (NIST) requirements. The results of our limited scope review, presented below and in the attached reporting template, will be combined with those of other Agency Inspectors General and used by the PCIE to prepare a report on the status of PII protections within the executive branch.

CONCLUSION AND OBSERVATIONS

Although the Department has made progress and has indicated that it plans to fully implement needed controls, our review found that recently developed PII policies were missing certain key components and that implementation was, so far, incomplete.

Departmental Efforts

The Department has taken several positive steps to protect PII. The Office of the Chief Information Officer (OCIO) issued Department-level guidance (DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, on July 20, 2006), establishing requirements for the protection of PII in all Federal and contractor operated information systems. Organizations controlled by each of the Department's Under Secretaries have also issued separate and complementary guidance designed to ensure that required protective measures are implemented. Work is underway to deploy these recently developed controls and include actions such as utilizing two-factor authentication for remote access and installing encryption capabilities on laptop computers.

Various program elements have also begun performing internal reviews to determine whether controls had been implemented and identify needed corrective actions. For instance, a review conducted by the Office of the Chief Financial Officer identified a number of activities that have been or will be taken to meet security requirements, including the installation of encryption software on all laptops and the development of a plan of action and milestones to bring all systems into compliance. In addition, the Office of Management completed a review of policies and processes to ensure that the Department had adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, PII. Although this management review did not include formal recommendations, it did identify certain areas that needed improvement.

Policies and Implementation

Even though the Department has developed policies for protecting PII that is transported or accessed remotely, this guidance was not complete. While each of the policies we reviewed prescribed certain controls for transporting PII, they did not always meet requirements established by NIST. For instance, several of the policies reviewed required that transported PII be encrypted; however, rules for determining whether the information should be transported at all were not defined. Other implementing instructions did not address issues such as controls necessary for ensuring that PII maintained on personal computers used for telecommuting is not exposed to compromise. Policies also did not always explicitly describe rules or prohibitions related to the remote download and/or storage of PII.

Based on limited testing, we also determined that the Department had not yet implemented all the protective measures recommended by OMB and/or required by NIST. For example, NIST required risk assessments had not always been updated to ensure that all PII, whose exposure could result in a moderate or high impact, had been explicitly identified. Specifically, the results of an internal review from one program disclosed that certification and accreditation documents, including risk assessments, had not been modified to address PII issues. In addition, the programs reviewed had not implemented logging of computer-readable data extracts from systems containing PII. Various officials told us that

while this step was recommended by OMB, they did not believe that it was practical. Furthermore, the field sites reviewed had either not developed policies addressing all OMB recommendations or had not yet completed implementation of established policies.

ONGOING ACTIVITIES

Although we have completed the tests specified by the PCIE (see attachment 2), our audit to evaluate the adequacy of the Department's protection of PII continues. During the coming months, we plan to visit additional field sites to determine whether facility contractors have implemented needed protective measures. At the completion of audit field work, we will issue a follow-on report which will contain formal audit recommendations, as appropriate.

We appreciate the cooperation of you and your staff during the conduct of this review.

Rickey R. Hass
Assistant Inspector General
for Financial, Technology, and Corporate Audits
Office of Inspector General

Attachments (2)

cc: Chief of Staff
Director, Policy and Internal Controls Management, NA-66
Team Leader, Audit Liaison, CF-1.2
Audit Liaison, IM-10
Audit Liaison, HR-1
Audit Liaison, EM-33
Audit Liaison, FE-3
Audit Liaison, SC-32.1

SCOPE AND METHODOLOGY

This review was performed between June and September 2006 at Department Headquarters in Washington, DC and Germantown, MD; the Oak Ridge Office, Oak Ridge National Laboratory, and Y-12 National Security Complex, Oak Ridge, TN; and the National Energy Technology Laboratory, Pittsburgh, PA and Morgantown, WV.

To satisfy PCIE review requirements, we:

- Reviewed Federal regulations and Departmental directives and guidance pertaining to personally identifiable information;
- Reviewed program level policies relevant to protecting personally identifiable information;
- Held discussions with program officials from Department Headquarters and field sites reviewed, including representatives from the Offices of the Chief Information Officer, Chief Financial Officer, Environmental Management, Fossil Energy, Management, and Science, as well as the National Nuclear Security Administration; and,
- Analyzed information provided by the organizations reviewed to determine compliance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, as well as compliance with the President's Council for Integrity and Efficiency guidance.

APPENDIX I: IG DATA COLLECTION INSTRUMENT - DEPARTMENT OF ENERGY

This data collection instrument (DCI) was developed by the FAEC IT Committee of the PCIE/ECIE to assist IGs in determining their agency's compliance with OMB Memorandum M-06-16. The data collection instrument contains three parts. The first part is based on a security checklist developed by NIST (see Section 1 below). Questions in the DCI are designed to assess Agency requirements in the memorandum, which are linked to NIST 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, IG's 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 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 and Tested" if documents have been examined & 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.

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
Procedure	*Yes* *No* *Partial* *Not Applicable*	*Controls Not Yet in Place* *Policy* *Procedures* *Implemented* *Monitor & Tested* *Integrated*
STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?	Partial	Controls Not Yet In Place
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	
Action Item 1.2: Has the Agency verified existing risk assessments?	Partial	

APPENDIX I: IG DATA COLLECTION INSTRUMENT - DEPARTMENT OF ENERGY

Comments: Not all Department organizations had insured categorization of systems containing PII in accordance with FIPS 199 or updated relevant risk assessments.		
Procedure	REQUIRED RESPONSE Yes No Partial Not Applicable	OPTIONAL RESPONSE Controls Not Yet In Place Policy Procedures
STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?	Partial	Policy
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	
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	
1. For Personally Identifiable Information physically removed:		
a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?	Partial	
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?	Partial	
2. For Personally Identifiable Information accessed remotely: a. Does the policy explicitly identify the rules for determining whether remote access is allowed?	Partial	
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?	Partial	
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.)	Partial	
Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?	Partial	
Comments: Not all Department organizations had established and/or updated policy regarding protection of PII, including safeguards over transport and remote access in accordance with OMB and NIST requirements.		

APPENDIX I: IG DATA COLLECTION INSTRUMENT - DEPARTMENT OF ENERGY

Procedure	REQUIRED RESPONSE Yes No Partial Not Applicable	OPTIONAL RESPONSE Controls Not Yet in Place Policy Procedures Implemented 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	Policy
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	
** 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?	Partial	
** Evaluation could include a review of remote site facilities and operations.*		
Comments: We found that not all of the field sites reviewed had ensured that personally identifiable information was adequately protected when being transported or stored offsite.		

APPENDIX I: IG DATA COLLECTION INSTRUMENT - DEPARTMENT OF ENERGY

If personally identifiable information is to be transported and/or stored offsite follow Action Item 4.3, otherwise follow Action Item 4.4

Procedure	REQUIRED RESPONSE Yes No Partial Not Applicable	OPTIONAL RESPONSE Controls Not Yet in Place Policy Procedures Implemented Monitor & Tested Integrated
STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?	Partial	Policy
Action Item 4.1: Have NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection been implemented by the Agency?	Partial	
** 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?	Partial	
** 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?	Partial	
Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?	Partial	
Comments: We found that not all Department elements reviewed had implemented adequate controls over remote access to personally identifiable information. Specifically, not all organizations had implemented two-factor authentication for remote access, monitored downloads of information from databases containing personally identifiable information, or ensured that remotely stored PII was encrypted.		
(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 - DEPARTMENT OF ENERGY

Section Two

Additional Agency Actions Required by OMB M-06-16	
Procedure	Yes No 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?	Partial
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
3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?	Yes
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?	No
Comments: We found that not all Department elements had encrypted mobile devices or received the necessary waivers at the time of our review. In addition, two-factor authentication had not been implemented at all organizations. We also found that none of the organizations reviewed were logging all computer-readable data extracts from databases containing sensitive information.	

APPENDIX I: IG DATA COLLECTION INSTRUMENT - DEPARTMENT OF ENERGY

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).

Review

Scope and methodology of work completed based on the PCIE/ECIE review guide Step 2 page 4.

The scope of our review was limited to reviewing Department programs and certain field sites. We reviewed relevant Federal regulations and Departmental guidance pertinent to protection personally identifiable information. We also met with officials from various Department programs and field sites to discuss safeguards over personally identifiable information. In addition, we evaluated policies and related implementation to determine compliance with OMB and PCIE direction.

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	C	C	C	C
Examinations (G/F/C)	G	C	G	G	F
Tests (independently verified - Y/N)	N	Y	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.

OSM Narrative: *Please address the coverage of your assessment, and include any comments you deem pertinent to placing your results in the proper context.*

Overall conclusion statement.

Although the Department has made progress and has indicated that it plans to fully implement needed controls, our review found that recently developed PII policies were missing certain key components and that implementation was, so far, incomplete.