



U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Security Over Personally Identifiable Information



Department of Energy
Washington, DC 20585

July 30, 2007

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Audit Report on "Security over Personally Identifiable Information"

BACKGROUND

Industry experts have reported that more than 100 million personal privacy records have been lost or stolen over the past two years, including information maintained by corporations, educational institutions, and Federal government agencies. In fact, over the past several years, the Department of Energy has experienced the loss of personal privacy records. On June 23, 2006, in response to security incidents involving the loss or compromise of sensitive personal information by several Federal agencies, the Office of Management and Budget (OMB) issued a memorandum recommending that agencies strengthen controls over the protection of Personally Identifiable Information (PII). OMB specifically required agencies to implement protections over PII developed by the National Institute of Standards and Technology (NIST), including those related to encryption, remote access, and risk assessments.

The Department of Energy maintains numerous information systems that contain PII. In response to a request from OMB, the Office of Inspector General, in coordination with the President's Council on Integrity and Efficiency, performed a review of the Department's controls over the protection of PII. The results of our preliminary review were provided to the Department on September 20, 2006, in our *Special Report on the Department's Security over Personally Identifiable Information* (OAS-L-06-20). Although the September 2006 report disclosed certain actions taken by the Department to safeguard PII, we expanded our review to determine whether the Department had effectively implemented safeguards for protection of PII.

RESULTS OF AUDIT

We found that the Department had not fully implemented all protective measures recommended by OMB and required by NIST. In particular, we observed that:

- Seven of eleven field sites reviewed (3 Federal, 8 contractor) had not identified information systems containing PII, or fully evaluated the risks of exposing PII stored in such systems;



- Controls for securing remote access to site-level systems containing personal information had not been fully implemented; and,
- Five sites had not identified mobile computing devices containing PII nor ensured that this information was encrypted as required by OMB.

We noted that not all OMB and NIST requirements had been incorporated in relevant Headquarters and site-specific policy documents. Even when policies were clear, programs and sites did not always enforce the requirements to ensure that all necessary controls were in place for protecting PII. Without improvements in policy development and implementation, the Department will have a difficult time securing personal information. In addition, there is a less-than-acceptable risk that affected individuals would not be notified if their personal information is exposed.

During our review, we recognized that the sheer volume of data processed within the Department of Energy complex made the protection of PII a significant challenge. We noted, as well, that the Department had taken positive steps to protect PII, including conducting internal reviews to determine whether adequate information protection safeguards were in place, and implementing additional controls for safeguarding PII. For example, a review conducted by the Office of the Chief Financial Officer at Headquarters identified a number of activities that have been or will be taken to meet security requirements. In addition, in March 2007, the Office of the Chief Information Officer and the Office of Management issued additional guidance reemphasizing user responsibilities for keeping laptop computers and the information they process more secure. Further, the Office of Science completed its updated Program Cyber Security Plan, the first such Department of Energy office to do so. Taken together, these actions will improve the Department's protection of personal information. Nonetheless, more remains to be done and we made several recommendations designed to improve security over PII maintained by the Department.

MANAGEMENT REACTION

Management concurred with the report's findings and recommendations. Management indicated that additional steps will be taken relative to our recommendations and believed that it is important that protection of sensitive information, including PII, be achieved as an integral part of the Department's cyber security program. In separate comments, the NNSA generally agreed with the report and indicated that a series of actions had been implemented to address our concerns. Management's comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Acting Administrator, National Nuclear Security Administration
Acting Under Secretary for Energy
Under Secretary for Science
Chief of Staff

REPORT ON SECURITY OVER PERSONALLY IDENTIFIABLE INFORMATION

TABLE OF CONTENTS

Personal Information Protection

Details of Finding	1
Recommendations	6
Comments	7

Appendices

1. Objective, Scope, and Methodology.....	8
2. Prior Reports	10
3. Management Comments	12

Personal Information Protection

Protection of Personally Identifiable Information

Protection of Personally Identifiable Information (PII) is a priority for both Federal and commercial organizations. Because of the significance of this issue, the Office of Inspector General performed reviews of protection measures over PII at Department of Energy (Department) Headquarters, seven national laboratories, and four other major Department sites.

As a result of our review, we determined that the Department had not implemented all protective measures recommended by the Office of Management and Budget (OMB) and required by the National Institute of Standards and Technology (NIST). Specifically, the Department had not identified all site-level systems containing PII or evaluated the risks associated with maintaining such systems; remote access protection measures had not been fully deployed in accordance with Departmental direction; and, sites had not identified mobile computing devices containing PII nor ensured that such information was encrypted.

Site-Level Systems

Seven of eleven field sites reviewed had not identified which site-level information systems contained PII. For instance, although the Pacific Northwest National Laboratory (PNNL) developed a list of certain systems believed to contain PII, such as the human resource system, the site had not finished reviewing all systems to verify whether they contained PII and whether the information was adequately protected. Similarly, officials at the Los Alamos National Laboratory (LANL) noted that, while they had identified all systems managed by the Information Systems and Technology Division that contained PII, there were a number of systems managed by other program areas at the laboratory that may contain personal information that had not been specifically identified or evaluated. We also found that although the Oak Ridge National Laboratory (ORNL) had begun to complete an inventory of all devices that contained PII, it had not conducted a review to identify all site-level systems that contained such information. In addition, the National Energy Technology Laboratory (NETL) had not identified its systems that contained PII, limiting its ability to ensure that data was protected at the appropriate levels.

Risk Assessments

Although NIST requires that databases containing PII be assessed for risk of improper exposure, seven sites and programs we reviewed had not evaluated or updated security plans to address the risks associated with maintaining PII. For instance, six systems maintained by a facility contractor at the Hanford Site were inappropriately protected at a low level of controls even though they contained PII. In addition, Headquarters officials from both the Office of the Chief Information Officer (OCIO) and the National Nuclear Security Administration (NNSA) commented that their respective organizations had not reviewed and updated risk assessments to ensure that protection of PII was appropriate. According to the NNSA official responsible for cyber security at Headquarters at the time of our review, a list of systems containing PII had not been developed by the program. As noted in our recent report on *Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007), the failure to conduct risk assessments limits the ability to analyze the nature and level of threats and vulnerabilities to a system.

Remote Access to PII

The Department had not fully implemented controls necessary to protect PII during remote access. In particular, two-factor authentication¹ or adequate Virtual Private Network (VPN)² time-outs for remote access to systems were not always implemented, and controls over information downloads had not been instituted – all necessary for ensuring secure remote access to information systems. Specifically, we found that Lawrence Berkeley National Laboratory (LBNL) and ORNL had not implemented the use of two-factor authentication for accessing all systems from a remote location even though many of these systems contained PII. Timeout functions – a period of inactivity after which a connection automatically terminates – for VPN remote sessions was 90 minutes at LBNL, three times the OMB recommendation of 30 minutes. Access to development systems at LBNL

¹ Two-factor authentication requires two independent ways to establish identity and privileges, such as both a physical device and a password, while traditional password authentication only requires knowledge of a password to gain access to a system.

² A VPN is a communications network that provides secure private communications over a non-private network.

which may contain PII also did not have remote access time-out functions activated. Furthermore, requirements for controlling downloads of PII to remote systems had not always been established at the sites reviewed. For instance, ORNL had not placed restrictions on the type of information that could be downloaded to remote computers. In addition, none of the programs or sites we evaluated logged and followed up on downloads of PII from systems, as recommended by OMB.

Encryption of PII

Although required by OMB, five of the sites we reviewed had not ensured that PII on all mobile devices was identified and encrypted. For instance, although Sandia National Laboratories developed policy for protecting PII, it had only begun the process of identifying PII on manager's laptops, which accounted for only about 11 percent of the more than 11,000 laptop computers needed to be reviewed at the site. We also found that LANL had started encrypting laptops if they knew they were going to be removed from the site, but had not encrypted the approximately 6,300 laptops not anticipated to be taken off-site. As noted in a recent Government Accountability Office report, encrypting data on mobile devices provides reasonable assurance that stolen or lost computer equipment will not result in personal data being compromised.

In addition, site officials had not taken affirmative action to ensure that encryption capabilities were utilized, where appropriate. For instance, at the time of our review, ORNL was not aware of the number of laptop computers that contained personal information and had not ensured that encryption capabilities were installed on all mobile devices. Although laboratory officials provided and made the use of encryption software optional, officials commented that they had no intention of mandating encryption until formally directed to do so via their contract. ORNL also had not received confirmation from users that PII was encrypted if it was maintained on a mobile device. In addition, neither Lawrence Livermore National Laboratory (LLNL) nor NETL had evaluated or received confirmation from users as to whether mobile devices contained PII, and had not ensured that encryption was utilized on all laptops. Further, most of the sites reviewed had not performed spot checks to verify user responses or ensure that appropriate

Security Policy and Program Direction

protections had been implemented. Absent knowledge of where PII is maintained and the deployment of encryption software to secure such data, the Department can not ensure that personal information is adequately protected.

These problems occurred because policies at Headquarters and sites reviewed did not address all OMB and NIST requirements. Even when policy had been developed, programs and sites had not always enforced requirements to ensure that all necessary controls were in place for protecting PII.

Policies

To their credit, various Department program elements and sites had developed policies and procedures for protecting PII. For instance, the OCIO issued Department-level guidance in July 2006 establishing requirements for the protection of PII in all Federal and contractor-operated information systems. In addition, organizations controlled by each of the Department's Under Secretaries have issued separate and complementary guidance designed to ensure that protective measures are implemented. For example, the Office of Science was one of the first Department programs to issue policy for protecting PII that applied to both Federal and contractor employees. However, the new Headquarters guidance was incomplete and the existing site-level policies had not been updated to reflect new requirements.

In particular, policies developed at Headquarters for protecting PII lacked certain critical elements. Specifically, the policies, including those issued by the OCIO, did not require the identification of all Headquarters or site-level systems containing PII that were maintained by both Federal and contractor officials as required by NIST. Although programs began to gather this information based on previously issued guidance, the effort remained incomplete. The policy also did not specifically require that relevant risk assessments be reviewed and updated, as necessary, to account for the protection of such information. Certain policies developed by Headquarters also did not explicitly address rules for downloading information, including whether or not it was permitted, or for utilizing personal computers for telecommuting – practices which could expose PII to unauthorized individuals outside of the workplace.

Sites had also not updated existing local policies to ensure protection of PII in accordance with OMB and NIST requirements. For example, at the time of our review, neither LBNL nor ORNL had updated policies to address requirements for protecting PII. Officials at ORNL commented that they did not anticipate developing such policy and having it fully implemented until Fiscal Year 2008. Although LBNL established a policy in March 2007, we found that the policy was incomplete and that the lab had not implemented Science program policy for all aspects of protecting personal information, such as the use of two-factor authentication for remote access to all systems. In addition, although certain contractors at the Hanford Site had maintained existing policies for protecting sensitive information, the policies did not specifically address, and were less stringent than, guidance set forth by OMB and NIST. Such policies did not require that PII be encrypted during storage or transmission, or that risk assessments be updated to reflect the protection of PII. PNNL's policies did not prohibit individuals from taking unencrypted laptops off-site and did not require that emails containing PII be encrypted. To its credit, PNNL took steps during our review to begin encrypting all laptops, culminating in the issuance of updated policy in March 2007.

Program Direction

Even when policies had been developed, programs and sites reviewed had not consistently or effectively enforced controls designed to protect PII. Officials, at various sites, stated that their respective programs had not been provided with adequate or timely guidance and therefore, they had taken independent action that they deemed appropriate, or delayed taking action altogether. For instance, at the time of our review, officials from several sites, including LANL and the Richland Operations Office, stated that although they had received general guidance from their respective programs regarding the requirements for protecting PII, specific requirements had not been provided. As such, the sites were unaware of the process for protecting PII consistent with Departmental requirements. Facility contractor officials at ORNL and the Hanford Site also commented that their compliance was not mandatory because the requirements for protecting PII had not been incorporated into their contracts. However, subsequent to our review, direction was provided to ORNL from the Department requiring protection of personal information on

mobile devices. Although most sites attempted to comply with OMB's recommendations for protecting PII, some sites downplayed its importance. For example, a cyber security presentation provided to us by one site indicated that the requirements surrounding PII were overly burdensome and should not be considered a high priority.

Information Security and Assurance

Until protective measures are fully implemented, the Department may have difficulty protecting personal information. Specifically, sites cannot implement the necessary security measures until they identify which systems contain PII. In addition, personal information stored on a lost or stolen mobile computing device is at increased risk of being obtained and misused by nefarious individuals because sites have not fully utilized encryption software. Furthermore, sites' failure to determine whether devices contain PII will likely mean that affected individuals would not be notified if personal information was exposed, thus making it impossible for them to take timely action to minimize possible negative effects. The need to know the location of PII was highlighted in an October 2006 Congressional report on *Agency Data Breaches Since January 1, 2003*, which disclosed that the failure of agencies to track all possible losses of personal information makes it difficult to know what data was lost or how many individuals were impacted.

RECOMMENDATIONS

To address the issues identified in this report, we recommend that the Acting Administrator, NNSA, the Acting Under Secretary for Energy, and the Under Secretary for Science; in coordination with the Department and NNSA Chief Information Officers:

1. Update Departmental and site-level policies for protecting PII to include applicable OMB and NIST requirements;
2. Implement OMB and NIST requirements for protecting PII on systems, to include updating risk assessments and executing adequate remote access procedures; and,
3. Verify that PII on mobile computing devices is identified and adequately protected by performing random checks to ensure data is encrypted.

**MANAGEMENT
REACTION**

Management concurred with the report's findings and recommendations and indicated that steps will be taken to further enhance the security of PII. Specifically, the Department plans to update existing policies and cyber security plans to provide sufficient protection of sensitive information. In addition, the OCIO plans to monitor the progress of the Department in verifying that PII on mobile computing devices is identified and adequately protected.

The NNSA generally agreed with the report and indicated that a series of actions had been implemented at each of its sites to address the issues identified in our report. NNSA disagreed with our recommendation to identify PII contained on mobile devices, but indicated that it had adopted a more conservative approach and assumed that all mobile devices contained PII and protected them accordingly.

**AUDITOR
COMMENTS**

Management's comments are responsive to our recommendations. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

To determine whether the Department of Energy (Department) had effectively implemented safeguards for protection of personally identifiable information.

SCOPE

The audit was performed between June 2006 and April 2007 at Department Headquarters in Washington, District of Columbia and Germantown, Maryland; the Lawrence Livermore National Laboratory, Livermore, California; the Lawrence Berkeley National Laboratory, Berkeley, California; the Oak Ridge Office, the Oak Ridge National Laboratory, and the Y-12 National Security Complex, Oak Ridge, Tennessee; the Sandia National Laboratories and National Nuclear Security Administration Service Center, Albuquerque, New Mexico; the Los Alamos National Laboratory, Los Alamos, New Mexico; and the National Energy Technology Laboratory, Pittsburgh, Pennsylvania and Morgantown, West Virginia. We also obtained information from the Richland Operations Office, the Office of River Protection and the Pacific Northwest National Laboratory, Richland, Washington.

METHODOLOGY

To accomplish our audit objective, we:

- Reviewed Federal regulations and Departmental directives and guidance pertaining to protecting personally identifiable information;
- Reviewed prior reports issued by the Office of Inspector General;
- Reviewed program and site level policies relevant to protecting personally identifiable information;
- Held discussions with program officials from Department Headquarters and sites reviewed, including representatives from the Office of the Chief Information Officer, the Offices of the Chief Financial Officer, Human Capital Management, Environmental Management, Science, and Fossil Energy, as well as the NNSA; and,
- Analyzed information provided by the organizations reviewed to determine compliance with OMB memorandum M-06-16, *Protection of Sensitive Agency Information*.

Appendix 1 (continued)

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Accordingly, we assessed internal controls regarding the safeguards of personally identifiable information across the Department. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We also assessed performance measures in accordance with the *Government Performance and Results Act of 1993* relevant to safeguards over PII. Although we did not identify measures specific to protecting PII, we noted that limited measures did exist related to cyber security. We did not rely on computer-processed data to satisfy our audit objective. Both the Department and NNSA waived the exit conference.

PRIOR REPORTS

- *Management Challenges at the Department of Energy* (DOE/IG-0748, December 2006). The Office of Inspector General (OIG) identified seven significant management challenges facing the Department of Energy (Department), including cyber security. In addition, the OIG identified a "watch list" of emerging issues that warrant continued attention. The report noted that although the Department had taken a number of positive steps in Fiscal Year 2006 relevant to cyber security, weaknesses still existed relating to logical access, establishing a complex-wide inventory of information systems, and implementation of an effective certification and accreditation process.
- *Special Report on The Department's Security over Personally Identifiable Information* (OAS-L-06-20, September 2006). Department and site policies for protecting personally identifiable information (PII) were missing certain key components and implementation was incomplete. Specifically, while each of the policies reviewed prescribed controls for transporting PII, requirements established by the National Institute of Standards and Technology (NIST) were not always met. Additionally, the Department had not implemented all protective measure recommended by Office of Management and Budget and required by NIST.
- *Internal Controls for Excessing and Surplusing Unclassified Computers at Los Alamos National Laboratory* (DOE/IG-0734, July 2006). The Los Alamos National Laboratory (LANL) had not complied with internal controls, implemented by both the site and the Department, when excessing and surplusing computers. Specifically, LANL did not sanitize the hard drive of a computer prior to processing the computer as excess/surplus, nor was the hard drive removed prior to transferring the computer for sale at auction. The failures in these internal controls raised concerns as to whether other recently released computers were sanitized and hard drives removed prior to being sent to auction. Given the potential sensitivity of data residing on the Department's systems, including its unclassified systems, it is important that formal excessing procedures be carefully followed.
- *Internal Controls over Personal Computers at Los Alamos National Laboratory* (DOE/IG-0656, August 2004). Weaknesses were identified that undermined confidence in LANL's ability to assure that computers were appropriately controlled and safeguarded from loss or theft; and that computers used to process and store classified information were controlled in accordance with existing property management and security requirements. Specifically, a number of classified desktop computers were not entered into the LANL property inventory; LANL's Office of Security Inquiries was not notified about a missing component of a computer system; and a listing of classified desktop and laptop computers was not accurate.
- *Special Inquiry on Operations at Los Alamos National Laboratory* (DOE/IG-0584, January 2003). LANL failed to take appropriate or timely action with respect to a number of identified property control weaknesses. Specifically, there was inadequate or

Appendix 2 (continued)

untimely analysis of, and inquiry into, property loss or theft and security issues; a lack of personal accountability for property; and, a substantial degree of dysfunction in the laboratory's communication and assignment of responsibilities for handling of property loss and theft concerns. LANL officials stated that incident reports did not indicate that reviews were completed as to the type of information contained on stolen equipment.

- *Inspection of Cyber Security Standards for Sensitive Personal Information* (DOE/IG-0531, November 2001). The Department did not always meet the requirements of the Privacy Act of 1974, the Freedom of Information Act (FOIA), or the Computer Security Act of 1987. Specifically, with regards to Privacy Act/FOIA personal information, the Department did not have baseline criteria for protection, nor did it group this information with other unclassified sensitive information for protection. Additionally, individual sites and program offices were allowed to develop differing security measures for protection of Privacy Act/FOIA personal information.



Department of Energy

Washington, DC 20585

July 20, 2007

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL
FOR FINANCIAL, TECHNOLOGY AND
CORPORATE AUDITS

FROM: THOMAS N. PYKE, JR. 
CHIEF INFORMATION OFFICER

SUBJECT: Response to Inspector General's Draft Report, IG-34
(A06TG036) (B), Security over Personally Identifiable
Information

The Department of Energy has reviewed the Inspector General's Draft Report, IG-34 (A06TG036) (B), Security over Personally Identifiable Information, dated April 26, 2007.

Thank you for the opportunity to comment on this draft report. We fully support the Inspector General's efforts to ensure adequate protection of personally identifiable information (PII). We appreciate recognition in the report of several of the positive steps that have been taken over the last year to improve the protection of personally identifiable information. I am encouraged that the rollout of protective measures for PII continues throughout the Department.

I believe it is important that protection of sensitive unclassified information, including PII, be achieved as an integral part of the Department's cyber security program. We began our special emphasis on protection of PII through my June 30, 2006, Memorandum for Heads of Departmental Elements in which I transmitted to the Department for action OMB Memorandum M-06-16, Protection of Sensitive Agency Information. We then codified this policy guidance in more formal direction, issued as DOE CIO Cyber Security guidance CS-38, Protection of Personally Identifiable Information, on July 20, 2006.

This guidance was broadened to cover sensitive unclassified information in DOE CIO Cyber Security guidance CS-38A, Protection of Sensitive Unclassified Information, including Personally Identifiable Information, dated November 2006. In addition, five other DOE CIO Cyber Security policy issuances are also directly relevant to protection of PII, consistent with OMB Memorandum M-06-16: CS-1, Management, Operational and Technical Controls Guidance; CS-2, Certification and Accreditation Guide; CS-3, Risk Management; and CS-14,



Printed with soy ink on recycled paper

Appendix 3 (continued)

Portable/Mobile Guidance; and CS-24, Remote Access Guidance. In addition, the Deputy Secretary signed a Memorandum for Heads of Department Elements on August 17, 2006, Designation of Authority to Determine Whether Data on Each Laptop Computer is Non-Sensitive.

These DOE cyber security policy issuances cover the first three recommendations of OMB Memorandum M-06-16 and the processes outlined in the Security Checklist attachment to that memorandum. We do not believe the fourth recommendation in that memorandum provides sufficient value in reducing risk relative to cost. We have expressed this concern to OMB several times and do not plan to mandate that it be adopted in general across the DOE complex. This is consistent with the direction we received from OMB on July 10, 2006, that we should "look at this overall issue" and "implement on the basis of a common sense approach."

RECOMMENDATIONS

Recommendation 1: Update Departmental and site-level policies for protecting PII to include applicable OMB and NIST requirements.

Management Decision:

Concur.

The Office of the CIO and the DOE Cyber Security Working Group will ensure that DOE cyber security policy direction is updated to provide sufficient protection of sensitive unclassified information, including PII. The DOE Cyber Security Working Group is in the process of updating all of the Department's cyber security guidance as the cyber security Technical and Management Requirements (TMR) documents required by Department Order 205.1A are created. Special attention is being given to ensuring that all applicable OMB direction and NIST guidance is integrated into these policy issuances. Each Under Secretary's Program Cyber Security Plan (PSCP) is required to follow these TMRs as they provide cyber security policy and implementation direction for each Under Secretary's organization, including the field. Site implementation plans and policies are based on these Under Secretary PCSPs. The TMRs will all be completed and issued no later than September 2007.

Recommendation 2: Take action to effectively implement OMB and NIST requirements for protecting PII on systems, to include updating risk assessments and implementing adequate remote access procedures.

Management Decision:

Concur.

All DOE organizations, including field sites, are required to follow the Under Secretary PCSPs. The PCSPs follow or will follow DOE cyber security guidance that requires review of risk assessments whenever a security significant change is made to the systems, including changes in system security categorization levels, as well as guidance on controls for remote access. All DOE organizations, including field sites, are required to implement cyber security protections as specified in the Under Secretary PCSPs. Special attention will be given by the DOE Cyber Security Working Group as the TMRs are completed to ensure that direction for risk assessment and remote access procedures is sufficient to ensure adequate protection of PII. The TMRs will all be completed and issued no later than September 2007.

Recommendation 3: Verify that PII on mobile computing devices is identified and adequately protected.

Management Decision:

The Office of the CIO (OCIO) will request that the Under Secretaries report by September 2007 on their implementation of the Deputy Secretary's August 17, 2006, memorandum, in which they were given the authority to determine whether data on each laptop computer is non-sensitive. The requested report will include progress in implementing DOE cyber security policies and direction for protection of PII.

Field implementation to protect PII is guided by the PCSP issued by each Under Secretary. DOE Order 205.1A includes a requirement that each Under Secretary monitor PCSP implementation effectiveness through site assistance visits, program reviews, reviewing the results of IG and HSS audits, compliance reviews, self-assessments, analyses or performance measurement criteria, peer reviews, and vulnerability analyses.

Appendix 3 (continued)

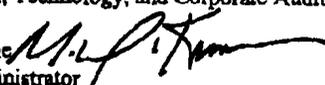


Department of Energy
National Nuclear Security Administration
Washington, DC 20585



May 22, 2007

MEMORANDUM FOR Rickey R. Hass
Assistant Inspector General
For Financial, Technology, and Corporate Audits

FROM: Michael C. Kane 
Associate Administrator
For Management and Administration

SUBJECT: Comments to Draft Personal Information Security Report;
Job Code A06TG036

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Security over Personally Identifiable Information." We understand that you have concluded that all protective measures that were recommended by the Office of Management and Budget have not been fully implemented and that you are making recommendations to update policies, implement requirements, and verify that information is identified and protected.

NNSA generally agrees with the report and, since the field work for this audit was completed, has implemented a series of actions at each of its sites that addresses the concerns raised by the IG. While we believe that we have met the intent of the IG's recommendations (encryption installed on devices that contain Personally Identifiable Information; removal of personal information from devices that are not equipped with encryption; restrictions of certain devices from leaving site boundaries or ensuring devices meet Federal standards), we disagree with the recommendation to verify that Personally Identifiable Information is on mobile computing devices. Rather, we believe that it is a more prudent course to assume that all mobile computing devices contain Personally Identifiable Information and protect them according to the national guidance and local directions. Equally, we believe that individuals that utilize Government issued computing devices that can be utilized in a travel/mobile environment are also fiscally accountable for those devices as well as the information contained therein should anything happen to those devices during the time that the devices are in a travel/mobile environment.

Should you have any questions related to this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: Linda Wilbanks, Chief Information Officer
David Boyd, Senior Procurement Executive
Karen Boardman, Director, Service Center



Printed with 50% fiber on recycled paper

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?
5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
<http://www.ig.energy.gov>

Your comments would be appreciated and can be provided on the Customer Response Form.