



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

Audit Report

Protection of the Department of
Energy's Unclassified Sensitive
Electronic Information

DOE/IG-0818


August 2009



Department of Energy
Washington, DC 20585

August 4, 2009

MEMORANDUM FOR THE SECRETARY

FROM: 
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Protection of the
Department of Energy's Unclassified Sensitive Electronic
Information"

BACKGROUND

The Department of Energy and its contractors store and process massive quantities of sensitive information to accomplish national security, energy, science, and environmental missions. Sensitive unclassified data, such as personally identifiable information (PII), official use only, and unclassified controlled nuclear information require special handling and protection to prevent misuse of the information for inappropriate purposes. Industry experts have reported that more than 203 million personal privacy records have been lost or stolen over the past three years, including information maintained by corporations, educational institutions, and Federal agencies. The loss of personal and other sensitive information can result in substantial financial harm, embarrassment, and inconvenience to individuals and organizations. Therefore, strong protective measures, including data encryption, help protect against the unauthorized disclosure of sensitive information.

Prior reports involving the loss of sensitive information have highlighted weaknesses in the Department's ability to protect sensitive data. Our report on *Security Over Personally Identifiable Information* (OIG-0771, July 2007) disclosed that the Department had not fully implemented all measures recommended by the Office of Management and Budget (OMB) and required by the National Institute of Standards and Technology (NIST) to protect PII, including failures to identify and encrypt PII maintained on information systems. Similarly, the Government Accountability Office recently reported that the Department had not yet installed encryption technology to protect sensitive data on the vast majority of laptop computers and handheld devices. Because of the potential for harm, we initiated this audit to determine whether the Department and its contractors adequately safeguarded sensitive electronic information.

RESULTS OF AUDIT

The Department had taken a number of steps to improve protection of PII. Our review, however, identified opportunities to strengthen the protection of all types of sensitive unclassified electronic information and reduce the risk that such data could fall into the hands of individuals with malicious intent. In particular, for the seven sites we reviewed:

- Four sites had either not ensured that sensitive information maintained on mobile devices was encrypted. Or, they had improperly permitted sensitive

unclassified information to be transmitted unencrypted through email or to offsite backup storage facilities;

- One site had not ensured that laptops taken on foreign travel, including travel to sensitive countries, were protected against security threats; and,
- Although required by the OMB since 2003, we learned that programs and sites were still working to complete Privacy Impact Assessments – analyses designed to examine the risks and ramifications of using information systems to collect, maintain, and disseminate personal information.

Our testing revealed that the weaknesses identified were attributable, at least in part, to Headquarters programs and field sites that had not implemented existing policies and procedures requiring protection of sensitive electronic information. In addition, a lack of performance monitoring contributed to the inability of the Department and the National Nuclear Security Administration (NNSA) to ensure that measures were in place to fully protect sensitive information. As demonstrated by previous computer intrusion-related data losses throughout the Department, without improvements, the risk or vulnerability for future losses remains unacceptably high.

In conducting this audit, we recognized that data encryption and related techniques do not provide absolute assurance that sensitive data is fully protected. For example, encryption will not necessarily protect data in circumstances where organizational access controls are weak or are circumvented through phishing or other malicious techniques. However, as noted by NIST, when used appropriately, encryption is an effective tool that can, as part of an overall risk-management strategy, enhance security over critical personal and other sensitive information.

The audit disclosed that Sandia National Laboratories had instituted a comprehensive program to protect laptops taken on foreign travel. In addition, the Department issued policy after our field work was completed that should standardize the Privacy Impact Assessment process, and, in so doing, provide increased accountability. While these actions are positive steps, additional effort is needed to help ensure that the privacy of individuals is adequately protected and that sensitive operational data is not compromised. To that end, our report contains several recommendations to implement a risk-based protection scheme for the protection of sensitive electronic information.

OTHER MATTERS

Our review also revealed that sites we reviewed were not encrypting sensitive data contained on desktops, servers and other network-based storage devices. This practice, currently in place or planned at certain Department of Defense activities to protect sensitive information, has been identified by NIST as a best practice and as part of an effective risk-based management approach to data protection. Our report, in Appendix 2, discusses the benefits and limitations of encryption for these types of devices and suggests additional actions that the Department may wish to consider.

MANAGEMENT REACTION

Management generally concurred with the report's recommendations and pledged to take action to address the weaknesses identified in our report. Management indicated that many of the issues identified in our report should be addressed as part of a risk-based approach to cyber security. In separate comments, the NNSA neither concurred nor disagreed with our specific recommendations. However, the NNSA did express concern over the practicality of utilizing encryption software in all situations and questioned the need to conduct Privacy Act Assessments.

As noted in the Management Comments section of this report (Appendix 4), the Office of Inspector General agrees that information technology restrictions and requirements should be risk-based and that the use of encryption software may be challenging in some circumstances. However, given the history of compromises of sensitive information both in the Department and in the Government at large, we concluded that an aggressive program of protecting information is in the best interest of the Department, its Federal and contractor personnel, and national security.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary of Energy
Under Secretary for Science
Chief of Staff
Chief Information Officer
Director, Office of Management

REPORT ON PROTECTION OF THE DEPARTMENT OF ENERGY'S UNCLASSIFIED SENSITIVE ELECTRONIC INFORMATION

TABLE OF CONTENTS

Protection of Unclassified Sensitive Electronic Information

Details of Finding	1
Recommendations.....	7
Comments	8

Appendices

1. Objective, Scope, and Methodology.....	13
2. Other Matters for Consideration	15
3. Prior Reports	16
4 Management/Auditor Comments.....	18

PROTECTION OF UNCLASSIFIED SENSITIVE ELECTRONIC INFORMATION

Ensuring Security of Sensitive Information

The Department of Energy (Department or DOE) had made improvements in implementing protective measures over personally identifiable information (PII) and had implemented certain recommendations made in our report on *Security Over Personally Identifiable Information* (DOE/IG-0771, July 2007). Our current review, however, established that additional action was needed to better protect all types of unclassified sensitive information, to include official use only and unclassified controlled nuclear information. In particular, the Department had not ensured that sensitive data on mobile devices, transmitted using email, or sent offsite using backup media, was encrypted, as appropriate. In addition, one site we visited had not implemented appropriate measures to protect sensitive information taken on foreign travel. Sites were also still working to complete required Privacy Impact Assessments (PIAs) for all systems containing privacy information.

Encryption of Sensitive Data

Sites reviewed had not always ensured that sensitive information maintained on mobile devices was encrypted. In addition, they did not always encrypt sensitive information transmitted using email or sent offsite using backup media. In particular, three sites had not always encrypted sensitive data maintained on laptop computers to protect against unauthorized disclosure, as required by Department and Federal directives. Although identified as a best practice by the Department and the National Institute of Standards and Technology (NIST), we found that full-disk encryption had only been deployed on approximately 6,000 laptops believed to contain PII at Sandia National Laboratories (SNL). Officials at SNL told us, however, that they had not implemented such measures for the remainder of the site's approximately 12,000 laptops even though they assumed that all laptops maintained by the site contained sensitive information.

SNL officials told us that the site had no plans to implement full-disk encryption on the remaining laptops that were assumed to contain other types of sensitive information such as official use only and unclassified controlled nuclear information. Officials noted that they also relied on file-level encryption software to protect sensitive data that was not PII, a practice with which we do not take issue. However, there was no assurance that all

users had this software as it was not part of the standard suite of installed software. As an example of the risk of harm associated with not encrypting data on mobile devices, in one recent incident, SNL reported that an unencrypted laptop containing sensitive data was stolen, potentially exposing the information contained on the device.

Lawrence Livermore National Laboratory (LLNL) officials also assumed that each of the laboratory's approximately 7,000 laptops contained some form of sensitive information, but they had not evaluated or confirmed that computers containing sensitive data were appropriately secured. Although LLNL developed a plan to install full-disk encryption software on approximately 2,500 laptop computers expected to be taken offsite, officials commented that they had not yet begun to implement this initiative due to funding limitations. In addition, we noted that because of the limited scope of the site's encryption plan, less than half of the total laptops used at the site are to be protected.

We also found that sensitive information transmitted via email or sent offsite using backup tapes was not always encrypted at several sites. For instance, SNL site-level policy did not require users to encrypt emails containing sensitive data when sent within the internal network even though encryption in these circumstances was required by both Department directives and the National Nuclear Security Administration (NNSA) policy. Although a SNL cyber security official commented that compensating network controls, such as firewalls and routers, were in place on the internal network to protect such transmissions from unauthorized disclosure, the Sandia Site Office's Designated Approving Authority believed these controls did not adequately mitigate the risk and that all emails containing sensitive unclassified information should be encrypted. To its credit, SNL officials commented that they had implemented encryption capabilities to protect email transmissions and updated site-level policy after our site visit.

While not every email or backup media must be encrypted, DOE Manual 205.1-7 – *Security Controls for Unclassified Information Systems Manual* requires that "...all SUI [Sensitive Unclassified Information] on all portable/mobile devices and removable media, such as CDROMS or thumb

drives containing SUI/PII must be encrypted." In addition, Office of Management and Budget (OMB) Memorandum 06-16 – *Protection of Sensitive Agency Information* directed that, "In those instances where personally identifiable information is transported to a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form."

However, we found that backup tapes at LLNL and the Pacific Northwest National Laboratory (PNNL) were not always encrypted in accordance with Department and program directives. Specifically, we noted that although both LLNL and PNNL sent their backup tapes offsite, they did not encrypt the contents of those backups before turning them over to their archive/storage subcontractors. Because LLNL officials assumed that all of their systems contained sensitive information, we believe that the backup tapes should have been encrypted in accordance with Department and OMB requirements. Although PNNL officials did not make the same assumption, they had not ensured that sensitive data was not contained on the tapes or was appropriately secured.

Laptops on Foreign Travel

Laptop computers taken on foreign travel by users at LLNL were not adequately protected against cyber security threats. In August 2007, the Directors at each of the NNSA's three weapons laboratories agreed to implement a pool of common laptops specifically configured and managed for use on foreign travel. However, more than one year later, LLNL had not yet implemented this approach. Based on our sample of ten users who took their laptops on foreign travel, including individuals that traveled to sensitive foreign countries, we found that only six of them had encryption capabilities on their laptops and only one of those users utilized full-disk encryption. Although LLNL laptops taken on foreign travel were physically inspected upon return, logical security assessments of computers to determine whether they had been tampered with or potentially infected with malware were not completed. In one case, we noted that a user connected his laptop to the LLNL network after he returned from travel but before taking his computer to the security organization for physical inspection, thereby subjecting LLNL to potential exploitation if the laptop had been compromised.

While we noted that the use of encryption was restricted by certain countries, compensating controls such as assessing computers for security breaches immediately upon return to the laboratory and prior to reconnection to the site network could help ensure protection against the introduction of malware into the LLNL computing environment.

Privacy Impact Assessments (PIAs)

PIAs are documents approved by the Senior Agency Official for Privacy and are used to determine the risks of collecting, maintaining, and disseminating privacy data in an electronic information system and ensuring that controls are in place to protect such data. To support the development of PIAs, the Department's Office of Management issued *Department of Energy Procedures For Conducting Privacy Impact Assessments* in 2007 which stated that PIAs were to be conducted "...on all systems that contain or administer information in identifiable form about its employees, contractors or members of the public." This guidance was formalized in January 2009 with the issuance of DOE Order 206.1 – *Department of Energy Privacy Program*

While we recognize that it takes time to develop PIAs, we noted that assessments were not completed for at least 14 systems (including 3 Federal systems) at 4 of the 7 sites reviewed. For instance, the NNSA Service Center had not completed any PIAs because officials stated that they did not have any PII in systems that were externally facing¹. In another case, SNL had interpreted the guidance to mean it only had to perform PIAs on systems that collected information about members of the public, not information collected on employees and contractors. SNL officials stated they had not developed PIAs for any of their systems because they did not collect information about members of the public. Nonetheless, we noted that information was manually collected and then stored in a number of information systems by SNL officials for various Federal purposes such as tracking foreign national visitors. In contrast to these examples, the Department's Chief Privacy Officer noted that the Department makes no distinction between whether a system is internally or externally facing when determining whether to complete a PIA. Effective

¹ Externally facing systems are those that are maintained by the Department and its contractors, but can be accessed by the public. Internally facing systems are systems that are only accessible by Department and contractor personnel.

implementation of the PIA process should help the Department ensure that privacy protections are considered and implemented through the life of an information system.

**Program
Implementation and
Performance Monitoring**

We found that Headquarters programs and field sites had not fully implemented existing policies and procedures that require sensitive electronic data be properly secured. A lack of performance monitoring contributed to the Department's inability to ensure that adequate protections were in place.

Program Implementation

Headquarters programs and sites reviewed had not fully implemented policies and procedures for ensuring that sensitive electronic information was protected. In particular, Technical and Management Requirement 22 and DOE Manual 205.1-7, issued by the Office of the Chief Information Officer (OCIO), required encryption of all sensitive unclassified data residing on mobile computing devices. However, we noted that sites had not fully implemented this policy and had not taken action to implement encryption of all mobile devices such as backup tapes. Furthermore, LLNL had not implemented stringent requirements for taking sensitive data on foreign travel because NNSA policies did not require that such action be taken.

Although OMB directed in September 2003 that agencies conduct PIAs for electronic information systems, the Department had not, until recently, issued a formal policy requiring PIAs for all systems containing privacy information. While the Department's Office of Management issued the *Department of Energy Procedures For Conducting Privacy Impact Assessments* in 2007, that stated that PIAs should be completed for all systems containing privacy information, this guidance had not been formalized into policy until after our review and was not included in site-level contracts. As such, officials at a number of sites reviewed commented that they were not required to follow the guidance. Lacking specific implementation direction, contractors had inconsistently interpreted OMB direction.

Even though NNSA program policy referred to the OMB direction as a requirement, NNSA's policy specifically excluded systems that were only accessible internally. The

Department's Chief Privacy Officer stated that in July 2008, NNSA officials agreed to develop PIAs for all systems containing PII, but our review of three NNSA sites disclosed that the sites had no plans to develop additional assessments. Subsequent to our field work, the Department issued DOE Order 206.1 that formally required a PIA for all unclassified systems containing federal employee and contractor privacy data, as well as information on members of the public. When fully implemented, this directive should help the Department ensure that systems containing privacy information are adequately assessed for protective measures.

Performance Monitoring

Headquarters programs and sites reviewed had not effectively implemented performance monitoring activities to ensure that sensitive electronic information was adequately protected. For instance, even though management agreed with a recommendation in our previous 2007 report on *Security over Personally Identifiable Information*, Department officials perform random checks to verify that PII on mobile computing devices was encrypted, none of the sites reviewed had instituted such a process. In SNL's case, officials had not ensured that all individuals even had the capability to encrypt sensitive data. Specifically, we noted that SNL maintained only 6,956 file-level encryption software licenses for nearly 12,000 members of the workforce despite the fact that officials assumed that every computer contained sensitive information. Furthermore, even though users at PNNL were responsible for installing encryption software, because it was not part of the standard suite of software, site officials did not perform reviews to determine whether users had actually installed the software. To their credit, the two Office of Environmental Management sites reviewed had ensured that full-disk encryption was installed on all laptops, effectively eliminating the need to conduct random inspections.

We also found that NNSA monitoring procedures did not detect nearly 1,300 laptops at SNL that were not encrypted because the site did not consider them mobile devices. We had previously identified this weakness within NNSA in

our 2007 report on *Security Over Personally Identifiable Information* and Headquarters cyber security officials told us that all laptops should be considered mobile devices and protected through encryption.

Information Security and Assurance

Without improvements to ensure adequate controls are in place, the Department may have difficulty protecting its sensitive electronic information, including PII. Specifically, the failure to encrypt all sensitive data maintained on mobile devices or transmitted using email or backup media could result in its unnecessary exposure of privileged data. For instance, the sites reviewed reported more than 240 computers lost or stolen during the last two fiscal years. However, none of the sites could ensure that sensitive unclassified information was protected on those machines through the use of encryption software. In addition, the importance of protecting sensitive data transported offsite using mobile media was highlighted when PII of 59,000 former employees at one of the Department's national laboratories was recently lost during a shipment as part of the Department's Former Worker Medical Screening Program.

The threat to sensitive information is not limited to external sources, as noted in a U.S. House of Representatives Committee on Government Reform report – *Agency Data Breaches Since January 1, 2003*, which indicated that the vast majority of data losses arose from physical thefts of computer equipment or unauthorized use of data by employees. Although encryption does not provide absolute assurance that sensitive data will not be exposed, it should enhance the Department's ability to ensure that data residing on lost or stolen equipment will not be compromised. The need for a strong risk-management program regarding sensitive data also becomes apparent when one considers that industry experts report that the number of cyber security threats continue to increase significantly each year.

RECOMMENDATIONS

To address the issues identified in this report, we recommend that as part of a risk-based sensitive data protection approach, the Administrator, NNSA, Under Secretary for Science, and Under Secretary of Energy, in coordination with the Department and NNSA Chief Information Officers:

-
1. Ensure that sensitive information on mobile devices, transmitted using electronic mail, or sent to offsite backup storage is adequately protected through encryption;
 2. Ensure that sensitive information maintained on mobile computing devices taken on foreign travel is adequately protected and that such devices are physically and logically examined prior to reconnection to government networks; and,
 3. Verify that sensitive data on computing devices is identified and adequately protected by performing random checks.

We also recommend that the Administrator, NNSA, the Under Secretary for Science, and the Under Secretary of Energy, in coordination with the Senior Agency Official for Privacy and Chief Privacy Officer:

4. Complete required PIAs on systems that contain privacy information.

MANAGEMENT AND AUDITOR COMMENTS

Management generally concurred with the report's findings and with the first three recommendations. Management fully concurred with recommendation four. In addition, management indicated that it planned to address a number of the issues identified in our report in future Department-level cyber security direction. In separate comments, the NNSA did not specifically indicate whether it agreed with our recommendations. To that extent, we consider NNSA's comments to be non-responsive. Responses from both Department and NNSA management indicated concerns with a number of assertions made in our report. We have addressed management's comments below and made technical changes to the report, as appropriate. Management's comments are included in their entirety in Appendix 4.

Management commented that if adequate steps were taken to ensure that there was no sensitive information on laptops or other mobile devices at a site, this determination should suffice without requiring encryption of all data on such devices. Management believed that this approach should help to balance risk against the cost and productivity loss associated with unnecessary use of encryption where its use

is not needed. Although we agree that it may not be necessary to encrypt mobile devices if they do not contain sensitive data, the sites reviewed had not identified which machines contained such information but instead assumed that all computers contained sensitive information.

Management commented that the type of protection provided for mobile computing devices taken on foreign travel should be determined by a local risk analysis. Management believed that upon return to a government site from foreign travel, it would be prudent to logically scan the device either before it is connected to a government network, or if connected, before it is given full access to the network. We agree that sites should be able to implement security requirements using a valid and documented risk analysis. However, an analysis of the need for conducting logical scans was not completed at LLNL – the site identified in the report as having security deficiencies related to laptops taken on foreign travel. Furthermore, as noted in the report, LLNL had not yet implemented a common pool of laptops for foreign travel as agreed to by the Directors of the three NNSA laboratories.

Management noted that performing random checks on computing devices to ensure encryption of sensitive data may be helpful, but noted that consideration of the need to perform random checks should be based on local risk analysis. Although we agree that risk-based decisions should be made at the site-level, none of the sites visited had instituted such a review process or documented reasons for not doing so. In our opinion, absent the use of full-disk encryption software, it is imperative that some sort of verification be performed to ensure users are appropriately encrypting sensitive data. Management also had previously agreed to perform such checks and noted its agreement in its response to our report on PII protections.

Management also expressed concern about the information included in Appendix 2 of our report. In particular, management indicated that consideration should be given to an analysis of performance, productivity, and cost when deciding whether to implement encryption of data at rest. Management's comments also indicated that there did not appear to be a Federal government-wide decision or recommendation that sensitive data on desktops or servers should be encrypted. Although we agree that no government-wide mandate existed to encrypt sensitive data

at rest, NIST discussed the benefits of this practice in NIST Special Publication 800-111 – *Guide to Storage Encryption Technologies for End User Devices*. Our report included a discussion of both the positive and negative aspects of encrypting data at rest that programs and sites should consider when implementing their information security programs.

In separate comments, the NNSA responded that while the term "sensitive electronic information" had no formal definition, three types of sensitive information were discussed in the report including official use only, PII, and unclassified controlled nuclear information. The NNSA noted that the protection requirements for each type of information arise from different legal authorities and require protections that differ significantly. Management also commented that our report did not appear to completely address or identify whether the Department and its contractors adequately protected "sensitive electronic information." In our report, we used "sensitive electronic information" to refer to various types of sensitive unclassified information as defined in Technical and Management Requirement 22, DOE Manual 205.1-7, and NNSA Policy Letter 14.2-C – *NNSA Certification and Accreditation (C&A) Process for Information Systems*. All three sources identify official use only, PII, and unclassified controlled nuclear information as examples of sensitive unclassified information. While we agree that the legal authorities and protection requirements may differ among the different categories, the issues we identified and our recommended corrective actions are applicable to all three types of sensitive electronic data.

The NNSA commented that the audit appeared to have been performed against regulatory requirements for protection of PII on mobile devices, but that recommendations concerned protection of data at rest on servers and workstations. Our recommendations primarily discussed the need to protect sensitive data on mobile devices or in transit, not data at rest.

The NNSA indicated that statements in our report regarding the use of full-disk encryption on laptops at SNL appeared to take issue with the site for not implementing what is considered a best practice and not a requirement. Management also stated that the report did not identify the number of laptops that were actually identified as mobile or

portable. As discussed in our report, SNL did not provide encryption capability to all users as part of the standard suite of software. We do not take exception that SNL had not deployed full-disk encryption to all laptops, but that the site had not ensured all sensitive data was encrypted using either full-disk or file-level encryption. While we noted during discussions with site officials and a review of documentation obtained from the site that only about ten percent of laptops were not transported offsite, NNSA Headquarters cyber security officials believed that all laptops should be considered mobile devices and appropriately protected.

The NNSA commented that we did not confirm if PII was contained on LLNL backup tapes that were turned over to its archive/storage subcontractors. Officials also noted that NIST Special Publication 800-53 – *Recommended Security Controls for Federal Information Systems* DOE Manual 205.1-7 did not specifically require the use of encryption for sensitive information when transported to and stored at remote sites, but allowed approving authorities to utilize a risk assessment to guide the use of encryption and/or physical security controls in this instance. Although we did not confirm whether the backup tapes at LLNL contained PII, officials at the site told us that they operated under the assumption that all systems contained some form of sensitive unclassified information. Therefore, enforcement of DOE Manual 205.1-7 would require the site to ensure that "...all SUI [Sensitive Unclassified Information] on all portable/mobile devices and removable media, such as CDROMS or thumb drives containing SUI/PII must be encrypted." Furthermore, a site security official noted during our review that the failure to encrypt backup tapes at the laboratory was a weakness that the site should address in the future.

The NNSA noted that PIAs did not need to be developed for contractor systems that collect only contractor information. The NNSA also noted that our report did not identify whether the systems indicated in the report as not having a PIA were due for one, as policies require PIAs to be completed during development or the certification and accreditation process. Furthermore, the NNSA commented that the manual collection of PII did not require a PIA. We determined that DOE Order 206.1 required that PIAs be conducted on all systems that contain or administer information in identifiable form about its employees,

contractors or members of the public. We also noted that the requirement to complete a PIA was established in the E-Government Act of 2002. As such, all 14 of the systems identified in our report should have been certified and accredited at least once since that time and the need for a PIA recognized. Department directives also required that all unclassified systems have a Privacy Needs Assessment or PIA that must be reviewed and updated annually. Finally, while we agree that the manual collection of PII did not by itself require the development of a PIA, the example noted in our report identified that SNL was manually collecting PII and inputting that information into an online database, thereby creating the need for such an assessment.

Appendix 1

OBJECTIVE	To determine whether the Department of Energy (Department) and its contractors adequately safeguarded sensitive electronic information.
SCOPE	The audit was performed between July 2008 and April 2009 at Department Headquarters in Washington, DC, and Germantown, Maryland; the Lawrence Berkeley National Laboratory, Berkeley, California; the Lawrence Livermore National Laboratory, Livermore, California; the Sandia National Laboratories, New Mexico and National Nuclear Security Administration (NNSA) Service Center, Albuquerque, New Mexico; and the Richland Operations Office, Office of River Protection, and the Pacific Northwest National Laboratory, Richland, Washington.
METHODOLOGY	<p>To accomplish the audit objective, we:</p> <ul style="list-style-type: none">• Reviewed Federal regulations and Departmental directives and guidance pertaining to protecting sensitive electronic information;• Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office;• Reviewed program and site-level policies relevant to protecting sensitive electronic information;• Held discussions with program officials from Department Headquarters and sites reviewed, including representatives from the Offices of Management, the Chief Information Officer, Health, Safety and Security, Environmental Management, Civilian Radioactive Waste Management, Science, as well as the NNSA; and,• Interviewed employees at the sites visited to determine whether sensitive electronic information was adequately protected while on foreign travel.

We conducted this performance 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. 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* related to protecting sensitive electronic information. Although we did not identify measures specific to protecting sensitive electronic information, we noted that limited measures did exist related to cyber security. We did not rely on computer-processed data to satisfy our audit objective.

Management waived an exit conference.

OTHER MATTERS FOR CONSIDERATION

In addition to the weaknesses identified related to protecting unclassified sensitive electronic information discussed in this report, we also identified an additional area for consideration at the seven sites reviewed. Specifically, none of the sites reviewed had encrypted sensitive data at rest on desktops and servers even though this was identified as a best practice by the National Institute of Standards and Technology (NIST) and other industry organizations.

As part of an effective risk management process, NIST Special Publication 800-111 – *Guide to Storage Encryption Technologies for End User Devices* states that full-disk encryption can be used to protect all data on a device against loss or theft, and file or folder level encryption can be used to retain protection while the device is powered on for data that is more sensitive than the rest of the data. Although management's preliminary comments on our report indicated that sites had used a risk-based approach to determine that sensitive data at rest did not need to be encrypted, sites did not provide documentation supporting accepted risks when requested. While not providing absolute assurance that sensitive data could not be exposed, NIST and other industry sources have reported that encryption of sensitive data at rest is an integral part of a strong cyber security strategy. Certain Department of Defense activities recently initiated plans to implement NIST recommendations by requiring that all sensitive data at rest be encrypted.

While encryption of data at rest has a number of benefits, it also presents certain obstacles that should be considered. For instance, research has demonstrated that, in certain cases, encryption can cause a loss of functionality, slowed operation time, or decreased computer performance. In addition, implementing encryption technologies on data at rest may require a large investment in software and hardware, as well as the potential need for additional support costs. Furthermore, as stressed by certain program officials, encryption may not be useful where internal controls are weak or are circumvented by malicious attacks.

SUGGESTIONS FOR IMPROVEMENT

To help support a defense-in-depth strategy and decrease the risk of compromise to sensitive information, we suggest that the Administrator, National Nuclear Security Administration (NNSA), Under Secretary for Science, and Under Secretary of Energy, in coordination with the Department and NNSA Chief Information Officers:

1. Employ a documented, risk-based decision process to identify situations in which encryption of sensitive data at rest is appropriate.

PRIOR REPORTS

Office of Inspector General Reports

- *Management Challenges at the Department of Energy* (DOE/EIG-0308, December 2008). The Office of Inspector General (OIG) identified six significant management challenges facing the Department of Energy (Department), including cyber security. The report noted that although the Department had made improvements in its unclassified cyber security program, we continued to identify deficiencies, including problems relevant to certification and accreditation of systems, contingency planning, systems inventory, and segregation of duties.
- *Security Over Personally Identifiable Information* (DOE/EIG-0771, July 2007). The OIG determined that the Department had not identified all site-level systems containing personally identifiable information 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 personally identifiable information nor ensured that such information was encrypted.
- *Excessing of Computers Used for Unclassified Controlled Information at Lawrence Livermore National Laboratory* (DOE/OIG-0759, March 2007). The Lawrence Livermore National Laboratory's (LLNL) policies, procedures, and internal controls regarding the excessing of unclassified computers were not always consistent with applicable Department policies. As a result, LLNL did not ensure that stored data was properly removed from embedded memory devices, computer hard drives were adequately sanitized, and the sanitization of memory devices was properly documented.
- *Alleged Loss or Theft of Personally Identifiable Information at Pantex* (INS/DOE February 2007). The Pantex Plant had significant internal control weaknesses in the management and retention of I-9 forms. Three factors that contributed to Pantex's inability to locate 442 I-9 forms when requested were: the possible premature destruction of files, a misunderstanding of record retention requirements, and the possible failure of the management and operating contractor to verify employment eligibility for employees who transferred to Pantex from other sites.

Government Accountability Office Reports

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains (GAO-08-525, June 2008). The Government Accountability Office (GAO) reported that 24 major Federal agencies had implemented encryption and developed plans to implement encryption of sensitive information to varied extents. From July through September 2007, the major agencies collectively reported that they had not yet installed encryption technology to protect sensitive information on about 70 percent of their laptop computers and handheld devices. While all agencies had initiated efforts to deploy encryption technologies, none had documented comprehensive plans to guide encryption implementation activities such as

Appendix 3 (continued)

installing and configuring appropriate technologies in accordance with Federal guidelines, developing and documenting policies and procedures for managing encryption technologies, and training users.

Appendix 4



Department of Energy
National Nuclear Security Administration
Washington, DC 20585



June 25, 2009

MEMORANDUM (TO): Ricky R. Hass
Deputy Inspector General
for Audit Services

FROM: Michael C. Kane *Michael C. Kane*
Associate Administrator
for Management and Administration

SUBJECT: Comments to the IG Draft Report on Sensitive Electronic
Information, AOSTG0631DRJMS No. 2008-02007

The National Nuclear Security Administration (NNSA) appreciates the opportunity to provide comments to the IG's report, "*Protection of the Department's Sensitive Electronic Information*". I understand that this audit was initiated to determine whether the Department and its contractors adequately safeguarded sensitive electronic information.

NNSA has a number of concerns with the current structure of this report. The term "sensitive electronic information" has no formal definition and three types of sensitive information are discussed in the report (Official Use Only (DUO), Personally Identifiable Information (PII) and Unclassified Controlled Nuclear Information (UCNI)). The protection requirements for each type of information arise from different legal authorities and require protections that differ significantly. By combining these types of information together, the IG report does not appear to completely address or identify whether DOE and its contractors are adequately protecting sensitive electronic information.

Further complicating matters, the audit seems to have been performed against regulatory requirements requiring protection of PII on mobile devices, but recommendations concern protection of data on servers and workstations. It would be easier to resolve the IG concerns, if the recommendations are revised to address the protection requirements of each category of information separately.

Specific Comments on Topical Areas in Report

Encryption of Sensitive Data

The IG report states that the Department and NNSA identifies full-disk encryption as a best practice and goes on to further state, "...we found that full-disk encryption had only been deployed on approximately 6,000 laptops believed to contain PH at SNL even though site officials assumed that each of the approximately 12,000 laptops maintained

*



0011100
Printed with soy ink on recycled paper

by the site contained sensitive information." As written, this statement appears to take issue against Sandia National Laboratories (SNL) for not implementing what is considered a best practice and not a requirement. Additionally, the report does not identify the number of laptops out of the 12,000 cited were actually identified as mobile/portable (used or transported beyond the perimeter of the facility).

The third paragraph under this section goes on to identify that encryption was not always used in the transmission of sensitive information within the internal network via email or when sent off site on backup tapes and it goes on to quote SNL officials on the compensating controls in place and the DAAA stating that he believed that the compensating controls did not adequately mitigate the risk. The report does not clearly specify whether the SNL official was addressing the issue in whole or purely from an internal network perspective. Also, DOE Manual 471.3-1 allows the transmission of Official Use Only information by unencrypted email using a word processing file that is protected by a password.

The fourth paragraph talks about the DOE Manual 205.1-7 requiring encryption on all portable/mobile devices storing SUIVPII... and OMS Memorandum (6/16) directing that, "In those instances where personally identifiable information is transported to a remote site, implement NIST 800-53 security controls ensuring that information is transported only in encrypted form." However, the IG report did not confirm if PII was contained on the LLNL backup tapes that were turned over to their archive storage subcontractors.

NIST 800-53 does not specifically require the use of encryption for sensitive information when transported to and stored at remote sites. It allows approving authorities to utilize an organizational assessment of risk to guide the use of encryption and/or physical security controls in this instance. DOE Manual 205.1-7 restates these controls verbatim.

Laptops on Foreign Travel

The IG report states that laptop computers taken on foreign travel by users at LLNL were not adequately protected against cyber threats. However, the report does not acknowledge that encryption is controlled or restricted in many countries. Some countries ban, or severely regulate, the import, export, or use of this technology. Taking laptops with encryption software to these countries could risk imprisonment or laptop confiscation. The IG report does not identify if the countries visited exercised such restrictions. The IG report should identify if the countries visited exercised such laws.

Privacy Impact Assessments

The IG report cites DOE procedures on page 3 that PIAs were to be conducted on all systems that contain or administer information in identifiable form about its employees, contractors, or members of the public. However, NNSA has no legal authority to conduct PIAs on contractor systems storing information about contractors. The IG report does not identify if the systems cited were contractor systems collecting contractor information.

The IG audit began July 2008, prior to the issuance of the DOE Order, and was finished during April 2009. The IG report fails to identify if the 14 systems cited were due for a PIA as the policies require PIAs to be completed during development or Certification and Accreditation.

Although one section of the policy states, "...it will be the policy of DOE to conduct PIAs on all systems that contain or administer information in identifiable form about its employees ..." the section above states the requirements differently. The manual collection of PII does not require PIAs. The E-Gov Act only requires PIAs for electronic systems. According to the Privacy Act, its requirements apply specifically to records under the control of an agency that holds PHI about US citizens and lawful permanent residence and DOE does not extend Privacy Act requirements to cover Foreign Nationals. Additionally, the Contractor Requirements Document (CRD) in the Order was issued in January 2009 and provides specific contractor requirements.

As the CRD requires contractors at a minimum to comply with the Privacy Act, and take appropriate actions to assist DOE in complying with Section 2088 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives, the report did not mention if the systems reviewed were Federal systems or contractor systems with contractor-owned information or information that is collected and maintained for the Federal Government. The DOE requirements were specific as it applies to Federal systems but unless those requirements are included in the eRD they are not imposed on the contractor.

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

Appendix 4 (continued)



Department of Energy
Washington, DC 20585

June 30, 2009

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES
OFFICE OF THE INSPECTOR GENERAL

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

SUBJECT: Draft Inspector General Report on "Protection of the Department's Sensitive Electronic Information," IG-34 (A08TIG063)

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to provide comments on behalf of the Department to the Office of Inspector General's May 19, 2009, draft report on protection of the Department's sensitive electronic information. The Department recognizes the importance of providing adequate protection of sensitive electronic information, and we appreciate the Inspector General's attention to this important concern.

The DC Department's Chief Financial Officer has requested that the OCIO respond to the recommendations of this draft report, consolidating the Department's comments from the various Departmental Program offices, including comments from the Office of Science, the Office of Civilian Radioactive Waste Management, Environmental Management and Nuclear Energy.

Comments that address the specific recommendations of the draft report are included below, while technical comments on the draft report are included in the attachment to this memorandum.

Recommendation

Ensure that sensitive information on mobile devices is protected using electronic file or server backup storage is adequately protected through encryption.

We partially concur with this recommendation. If adequate steps are taken to ensure that there is no sensitive information on laptops or on all the laptops or other mobile devices at a site, this determination should suffice without requiring encryption of all data on such devices. This should help to balance risk against the cost and productivity loss associated with unnecessary use of encryption where its use is not indicated, including the use of alternatives, mitigating controls as appropriate. We will ensure that this topic is addressed adequately in future Department-level cyber security directions, taking into account OIG, DHS and other external government-wide direction that is in place at that time.



Appendix 4 (continued)

Recommendation 2

Ensure that sensitive information maintained on mobile computing devices taken for foreign travel is adequately protected and that such devices are physically and logically examined prior to re-connection to government networks.

We believe that the type of protection provided for mobile computing devices taken for foreign travel should be determined by local risk analysis. If no sensitive information is on the device, protection such as encryption is probably not necessary. When such a device is returned to a government site, we agree that it is a good idea to logically scan the device either before it is connected to a government network or when it is connected, before it is given full access to the network, but the decision as to whether to do so should be determined by local risk analysis. We will ensure that this topic is addressed adequately in future Departmental level cyber security direction, taking into account OMS and other external government-wide direction that is in place at that time.

Recommendation 3

Verify that sensitivity data on computing devices is identified and adequately protected by performing random checks.

While this might be helpful, providing "extra" protection consideration of the need to perform random checks should be based on local risk analysis that takes into account the cost and possible lost productivity that may result. The Department appreciates that the Inspector General, in its audits and evaluations, employs randomized selection techniques to select sites and systems to review, helping to ensure that adequate protection is in place, consistent with applicable policy.

Recommendation 4

Complete required ITAs on systems that contain privacy information.

We concur with this recommendation.

Attachment

Appendix 4 (continued)

Attachment to memorandum from Thomas N. Pyke, Jr. to Rickey R. Hass concerning draft Inspector General Report on "Protection of the Department's Sensitive Electronic Information," IG-34 (A08170063)

Please consider these technical comments on this draft report.

In the Performance Monitoring section, the first paragraph states "none of the sites reviewed had instituted such processes." At least one Environmental Management site indicated that they perform full disk encryption of all laptops, and they do not feel it is also necessary to check these laptops for sensitive information. It is not clear whether the report is suggesting that laptops be periodically checked to ensure that they are actually encrypted, to ensure that the encryption software/firmware is working as intended, or to determine that file/folder encryption, if used, is being used correctly. We are concerned that adequate protection be in place, based on risk as determined (both) and minimizing adverse impacts relative to cost and productivity.

In the Information Security and Assurance section, incident statistics are cited as evidence of a growing problem relative to data loss through equipment theft or loss, email transmission, or unauthorized use. Citing incident reporting data trends in this way can be misleading, since increased user awareness, changing reporting requirements, and deployment of improved monitoring and detection systems can contribute to increasing numbers of reports. As a result of these factors, this may not actually be a growing problem, as is stated in the report. Also, multiple program offices have noted that in the second paragraph of this section there is an inference that Idaho National Laboratory (INL) lost the Personally Identifiable Information (PII) of 59,000 employees. This paragraph should be corrected to clarify that another DOE organization was responsible for or involved in this exposure of PII, not INL.

We are also concerned about Appendix 2 of the draft report, Other Matters for Consideration. The draft report points out that none of the sites evaluated had implemented full disk encryption for data at rest, except for mobile devices, nor had the sites provided documentation supporting the accepted risks for potentially sensitive data not being encrypted at rest.

It appears that the Federal Government has made a top-level, risk-based decision that encryption is important for laptops and removable media that contain sensitive information. This is clear in OMB direction and NIST SP 800-111's reference to that direction. But there does not appear to be such a Federal Government-wide "decision" or recommendation that sensitive data on desktops or servers should be encrypted. There is possibly very serious performance, productivity and cost issues associated with consideration of this type of encryption, and the risks would have to be very high to overcome these concerns. Within our current DOE cyber security management structure, neither DOE nor any of the PESP owners have chosen to recommend or require consideration of encryption of sensitive data on desktops or servers. Of course, each DAA, in carrying out his or her C&A duties, addresses the risk associated with each system and the data on that system, and could choose to require this unusually aggressive type of control if he or she felt it to be necessary to reduce the residual risk associated with a system to an acceptable level, also taking into account performance, productivity, and cost.

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.

This page intentionally left blank.

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.