



U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Special Report


The Department of Energy's July
2013 Cyber Security Breach



Department of Energy
Washington, DC 20585

December 6, 2013

MEMORANDUM FOR THE SECRETARY

FROM: 
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Review of the "Department of Energy's July 2013 Cyber Security Breach"

BACKGROUND

To facilitate its administrative and operational needs, the Department of Energy maintains a substantial amount of personally identifiable information (PII). The Department's Management Information System (MIS) provides a gateway for users to access a system known as the DOE Employee Data Repository (DOEInfo) database. That system was implemented in 1994, and over time has become the central repository for information on the Department's current and former employees, dependents and contractors. Among other data elements, information stored in DOEInfo included name, address, Social Security number, date and place of birth, and banking information. In addition, Homeland Security Presidential Directive 12 badge and position sensitivity information, as well as security questions and answers necessary to request username and password resets, were stored in the database.

Over the past several years, MIS has been involved in no less than three cyber security breaches. According to Department officials, neither of the first two incidents, one in May 2011, and the second in January 2012, appeared to result in the loss of personal information. In July 2013, however, hackers exploited a software vulnerability to gain access to MIS and exfiltrated personal information from DOEInfo.

Because of the importance of ensuring the security of the Department's systems and sensitive information and at the request of the Chief Information Officer, we commenced a special review into the circumstances surrounding the MIS/DOEInfo breach. During our review, we conducted more than 35 interviews with Federal officials and contractor personnel from most of the Department's programs and staff offices. We also reviewed supporting information pertinent to MIS and DOEInfo and the events surrounding the breach.

RESULTS OF REVIEW

In spite of a number of early warning signs that certain personnel-related information systems were at risk, the Department had not taken action necessary to protect the PII of a large number of its past and present employees, their dependents and many contractors. We concluded that the July 2013 incident resulted in the exfiltration of a variety of PII on over 104,000 individuals.

Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. Compliance and technical problems included:

- The frequent use of complete Social Security numbers as identifiers, a practice contrary to Federal guidance. While not a direct contributor to the July 2013 breach, officials also failed to encrypt PII stored on the breached system, a practice that ignored a key industry and Federal best practice.
- Permitting direct internet access to a highly sensitive system without adequate security controls. Interestingly, routine internet access to e-mail required greater security than did access to the vast amounts of PII contained in DOEInfo.
- Lack of assurance that required security planning and testing activities were conducted. In particular, we determined that MIS and DOEInfo had not been securely integrated with one another. The Office of the Chief Information Officer (OCIO) also had not performed the required system certification testing or provided MIS an authorization to operate.
- Permitting systems to operate even though they were known to have critical and/or high-risk security vulnerabilities. The Department had not taken appropriate action to remediate known vulnerabilities on its systems either through patching, system enhancements or upgrades.
- Failure to assign the appropriate level of urgency to replacing end-of-life systems. Although core support for the version of the compromised application upon which MIS was built ended in July 2012, the Department did not purchase updated software until March 2013 – 8 months after support for the outdated application ended.

We also identified numerous contributing factors related to inadequate management processes. These issues created an environment in which the cyber security weaknesses we observed could go undetected and/or uncorrected. Specifically, we discovered:

- Competing priorities between mission-related work and cyber security that resulted in continued operation of systems even though they were known to have high-risk vulnerabilities. In that respect, officials told us that they lacked the authority to impose restrictions on system operation or take other corrective measures when known security vulnerabilities were not addressed. We could not determine with certainty whether the lack of authority, in all instances, was real or only perceived.
- Unclear lines of responsibility between and within program and staff offices. As it related to the July 2013 breach, officials from the Office of the Chief Financial Officer (OCFO) told us that they believed that the OCIO was responsible for patching vulnerabilities in the breached system. However, OCIO officials told us just the opposite, that the OCFO was responsible for that task.
- Lack of awareness by responsible officials regarding complete operating environment for the vulnerable database. We learned that since its deployment in 1994, over 30 separate

systems had become attached to DOEInfo. At least two of the interconnected systems were no longer being used, one of which had non-sensitive data taken from it during the breach.

- Ineffective communications and coordination among responsible officials. OCIO officials told us that various system owners they supported prohibited them from making security updates to applications in a timely manner because doing so would make it harder for employees to do their work. Conversely, program officials indicated that they directed security related issues to the OCIO and never received responses. We found that communication issues within the OCIO likely contributed to the recent breach. Specifically, system anomalies discovered by an application developer and reported to the OCIO prior to the breach were not fully investigated prior to being corrected. In this case, we question the thoroughness of Department's analysis of the reported anomalies.

While we did not identify a single point of failure that led to the MIS/DOEInfo breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease. The attackers in this case were able to use exploits commonly available on the internet to gain unfettered access to the relevant systems and exfiltrate large amounts of data – information that could be used to damage the financial and personal interests of many individuals. As noted, in many past Office of Inspector General Evaluation Reports completed pursuant to the *Federal Information Security Management Act of 2002*, weaknesses identical to those exploited in this case hold the potential for significant harm to the Department.

We also found that the extent of PII stolen was much more extensive than that originally reported by the Department. Alarming, we noted as many as 150,000 unique 9-digit records (possible Social Security numbers) in the forensic data gathered after the event. In response to our analysis and briefing to the Deputy Secretary in September 2013, the Department's Chief Information Officer and Acting Chief Financial Officer stated that they believed many of the records included in the forensic data represented false positives, but estimated the number of individuals impacted to be over 104,000. Breached information also exceeded just the names, dates of birth and Social Security numbers initially reported by the Department. In particular, the forensic data we analyzed also revealed that select bank account numbers, places of birth, education, security questions and answers, and disabilities were also included in the loss of information. Department officials told us that they examined the evidence we provided, validated it, and were in the process of notifying all impacted individuals that their PII had been compromised.

Financial and Program Impacts

In addition to the obvious risk to individuals whose PII was exposed, the financial consequences to the Department to recover from this breach of data security will be substantial. The OCIO noted that, as of October 2013, the Department estimated it would spend approximately \$1.6 million for credit monitoring and labor costs associated with establishing a call center through which affected individuals could obtain additional information on the breach. We noted that additional costs may be necessary to support continued call center operations. In addition,

the Department had incurred significant costs associated with the recovery and lost productivity – funds that could have been better spent supporting the Department's core missions. In particular, in October 2013, the Secretary authorized the use of up to 4 hours of administrative leave to all affected Federal employees to take action to correct issues associated with the event, an action we estimate could cost the Department an additional \$2.1 million in lost productivity.

Morale and reputational issues associated with the breach also have an adverse impact upon the Department. According to officials we spoke with, various employees received notification that their PII had been compromised in both this and an earlier unrelated breach and noted that employee complaints demonstrated a loss of confidence in Departmental cyber security. For those reasons, we believe that the Department needs to redouble its effort to improve its relationships with the affected individuals to ensure that notifications are made as quickly as possible.

Path Forward

Without improvements to the Department's information technology and management control environment in areas such as the use of Social Security numbers, internet accessibility, vulnerability management and continuous monitoring, the Department's systems containing sensitive information, including PII, remain at a higher than necessary risk of unauthorized disclosure. The Department moved to secure the compromised system subsequent to the July 2013 breach. However, we noted that it had identified other high-risk systems that could also be at risk of future compromise. These applications contain PII and protected health information, the loss of which could affect public safety and health.

The Department can begin to rebuild trust by revamping its Headquarters' cyber security program and control environment, enhancing communications and coordination in a number of areas related to cyber security and safeguarding PII, and moving away from the "stove piping" approach to managing information systems and data. To help address these issues, we made a series of recommendations designed to improve security over PII maintained by the Department.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had taken and/or initiated corrective actions. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in Appendix 4.

Attachment

cc: Deputy Secretary
Acting Under Secretary for Nuclear Security
Acting Under Secretary for Management and Performance
Acting Under Secretary for Science and Energy
Chief of Staff
Chief Information Officer
Acting Chief Financial Officer
Chief Health, Safety and Security Office

**SPECIAL REPORT ON THE DEPARTMENT OF ENERGY'S JULY 2013
CYBER SECURITY BREACH**

**TABLE OF
CONTENTS**

Technical Issues Contributing to the Cyber Security Breach

Details of Finding1

Recommendations9

Management Reaction and Auditor Comments10

Appendices

1. Timeline of Events Surrounding the Management Information System Security Breach.....11

2. Objective, Scope and Methodology12

3. Prior Reports13

4. Management Comments15

THE DEPARTMENT OF ENERGY'S JULY 2013 CYBER SECURITY BREACH

Technical Issues Contributing to the Cyber Security Breach

The Department of Energy (Department) assessed the Management Information System (MIS) and DOE Employee Data Repository (DOEInfo) database as moderate-risk systems according to the criteria set forth in Federal Information Processing Standard 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised. Although NIST required certain controls to be implemented to protect the systems, our review found that a number of these controls had not been implemented or processes were not in place to ensure that controls were operating effectively.

Use of Unencrypted Social Security Numbers

The Department inappropriately utilized Social Security numbers as an identifier in DOEInfo despite an Office of Management and Budget requirement that the use of Social Security numbers be eliminated to the extent possible by November 2008. Officials told us that the protection of personally identifiable information (PII) in several of the Department's systems had been considered as part of its response to the Office of Management and Budget requirement. The officials indicated, however, that DOEInfo was not one of those systems considered even though it was the Department's primary repository for storing PII. In addition, the database had not been constructed in a manner in which Social Security numbers were restricted to a minimum number of tables or otherwise obfuscated in the system. In particular, we noted that 354 of the 543 (65 percent) tables exfiltrated from the database contained Social Security numbers. Officials informed us that, since 2006, almost 70 tables had been added to the database using an identifier other than an individual's Social Security number. However, no efforts had been undertaken to eliminate the unnecessary use of Social Security numbers in the existing DOEInfo database tables even though the requirement to do so was over 5 years old. In preliminary comments on our report, the Office of the Chief Financial Officer (OCFO) stated that it had initiated actions following the July 2013 breach to reduce the number of Social Security numbers in the database, resulting in the removal of a number of tables.

Even though Social Security numbers were used, the sensitive data maintained in the DOEInfo database was generally not encrypted. Specifically, our analysis identified that none of the 354 tables containing Social Security numbers had encryption enabled. The encryption of data at rest is an industry best practice, which NIST noted should be considered as part of a defense-in-depth strategy to maintain the confidentiality and integrity of information. Although we recognize that encrypting data at rest may result in some performance issues, given the sensitivity of the information, we believe that encryption technologies should have been considered. We previously identified issues related to encrypting data at rest at various programs and sites in our report on *Protection of the Department of Energy's Unclassified Sensitive Electronic Information* (DOE/IG-0818, August 2009). In preliminary comments on our report, OCFO officials noted that encryption would not have protected the data in DOEInfo from the type of attack that occurred in July 2013. While this may be true, we continue to believe that encryption within the system could protect the Department's PII from a number of other types of attacks and is a worthwhile control implemented by other industry organizations.

Internet Accessibility

Access to the information within the DOEInfo database through the MIS gateway did not require the use of enhanced authentication mechanisms, such as two-factor authentication or a virtual private network. The use of two-factor authentication would have required a valid user to provide two means of identity proofing – such as a password, token or biometric signature – prior to accessing the system from the internet. Instead, only a user name and password were required to access MIS from any location with an internet connection. While we understand the need for individuals outside the Department's internal network to access certain information in DOEInfo, following a breach of MIS in January 2012, the OCFO's Director of Corporate Information Systems expressed concern that the system was directly accessible from the internet to various officials within the Office of the Chief Information Officer (OCIO), including the Chief Operating Officer, Chief Architect and former Chief Information Security Officer. In addition, during our review, OCIO and OCFO officials questioned why two-factor authentication had not been considered for MIS. We noted that, despite the concerns that had been raised, removal of MIS from the internet had not been given sufficient consideration.

Security Planning and Testing

We identified weaknesses related to system security planning and testing for both MIS and DOEInfo. For example, we noted that MIS and DOEInfo had not been securely integrated with one another. Specifically, the systems were owned by two different groups within the Department – the OCIO and OCFO respectively – and thus not included within the same authority to operate. While NIST noted that such an approach can provide a more targeted application of security controls within each system, we found that the Department's treatment did not relieve it of the responsibility to ensure that MIS and DOEInfo were integrated in a secure and functional manner. In addition, our review noted that, despite having been operable for almost 10 years, no security planning documentation had been completed for MIS. In particular, a security plan that provided details as to how required controls were implemented and/or inherited from other systems or the underlying infrastructure had been drafted in February 2013, but had not been finalized at the time of our review.

Despite being operational since 2004, the OCIO had not performed the required system certification testing or provided MIS an authorization to operate. As such, the system had been in operation for nearly 10 years without a thorough review of its security controls, including many of the controls that we determined were deficient, and the risks of operating the system in its untested state had not been identified. Although there was a significant gap in security, consideration had not been given to removing the system from the operating environment until such a time that controls were tested and risks appropriately addressed. As required by NIST, software applications such as MIS should be included in the risk management process because application security is critical to the overall security of the system. In January 2013, the OCIO acknowledged ownership of MIS and began efforts to appropriately authorize it for operation.

However, those efforts had not been completed at the time of the breach and remained incomplete at the time of our review. We also noted that MIS continued to operate on the Department's internal network even though security testing recently completed (testing report dated August 2013) by the OCIO identified nearly 80 required controls that were not fully

implemented. Documentation provided by program officials did not include support for mitigating controls to address these weaknesses and recommended that an authority to operate not be approved. At the time our report was issued, OCIO officials had not rendered a decision regarding authority for system operation.

Vulnerability Management and Continuous Monitoring

We found that the Department had not taken appropriate action to remediate known vulnerabilities in its systems either through patches, system enhancements or upgrades. Critical security vulnerabilities in certain software supporting the MIS application had not been patched or otherwise hardened for a number of years. Specifically, an operating system utility and a third-party development application that were installed on the MIS server had not been updated since early 2011. In addition, the vulnerability exploited by the attacker was specifically identified by the vendor in January 2013. As a system within the Headquarters environment, the OCIO was responsible for maintaining and patching the underlying infrastructure and the operating system on which MIS and DOEInfo operated. Further, although an upgrade for the application upon which MIS was built had been purchased jointly by the OCIO and OCFO in March 2013, it was not installed until after the breach occurred. The upgrade had been in the test environment since June 2013, but officials commented that it had not been applied to the operating environment because of functionality issues with an interconnected system. For the past 9 years, the Department's ongoing struggles with vulnerability management have been noted in our annual reports on the Department's unclassified cyber security program issued in accordance with the *Federal Information Security Management Act of 2002*.

The vulnerability management weaknesses identified above occurred because the OCIO had not implemented a robust continuous monitoring process over the operating environment that could have permitted identification and remediation of vulnerabilities in a timely manner. Although some level of scanning was conducted on the MIS system, it did not fully identify the vulnerabilities related to the compromised web application. Specifically, scans of MIS conducted by the OCIO in March and April 2013 identified the application installed on the server and several associated vulnerabilities, but action was never taken to mitigate the discovered problems. In addition, we noted that a more robust scanning capability, including the use of authenticated scanning, would have identified additional application-specific vulnerabilities within MIS. However, officials with the OCIO's Energy Information Technology Services group informed us that authenticated scanning had been attempted on MIS but failed for a variety of technical reasons. The Department's Office of Health, Safety and Security officials told us that they had been asked to complete an authenticated scan of the MIS and DOEInfo systems in support of the ongoing MIS certification process, but that the OCFO had indicated that DOEInfo did not need to be included in this effort.

Based on the results of our review, we continue to believe that such scanning, if performed simultaneously on both systems, could have made system owners in both the OCIO and OCFO aware of the level of vulnerabilities present on MIS and the potential effect of those on the information in DOEInfo. In preliminary comments to our report, OCFO officials indicated that scanning of both systems had been scheduled but not yet performed. As noted by NIST, agencies should establish effective continuous monitoring programs that include configuration management and control processes and assessments of security controls within and inherited by

each system. NIST also explained that justifications for not implementing patches should be documented, communicated and approved by appropriate management and warned that the risk of delaying remediation must be weighed carefully, considering the threat level, risk of compromise and consequences of compromise.

Lifecycle Management

The Department did not assign the appropriate level of urgency to replacing end-of-life systems. Specifically, core support for the version of the compromised application upon which MIS was built ended in July 2012, and the Department failed to purchase the extended support that would have provided limited coverage through July 2014. Although efforts were underway at the time of the breach to upgrade to a newer version of the application, the efforts had been slowed by technical difficulties with an interconnected application. During our research, we noted that since the time the application had been installed for MIS, an updated version of the same application had been introduced and withdrawn from the market and was now nearing the end of its core support period. Officials from the OCFO stated that a decision to upgrade the system had not been made until December 2012, because it had not reached the end of its useful life even though it was two iterations behind the current version. While we acknowledge the need to ensure responsible use of taxpayer funds, we question the decision not to upgrade to a less vulnerable version of the application sooner or give adequate consideration to how susceptible the system was to being breached and the criticality of information it contained.

In preliminary comments on our report, OCFO officials noted that the end-of-life for the compromised application was July 2014. However, our review determined that the software's core support period expired in July 2012, and an OCFO official confirmed that the extended support option had not been purchased. Under a risk-based approach to cyber security, we believe the Department should have considered the risks associated with continuing to operate an internet accessible system granting access to a large database of PII on an unsupported platform. Further, we believe that the Department should have considered costs associated with mitigating a system breach when considering the timing of lifecycle management activities for such systems. We noted the Department procured the updated version in March 2013 for approximately \$4,200. That amount coupled with labor costs associated with testing and installing the upgrade were significantly less than the cost to mitigate the affected system, notify affected individuals of the compromise of PII and rebuild the Department's reputation.

Contributing Factors to the System Breach and Subsequent Loss of PII

We identified a number of contributing factors that created an environment that permitted cyber security weaknesses to go undetected and/or uncorrected. In particular, we determined that issues related to competing priorities, unclear lines of responsibility, lack of urgency and awareness over cyber security, inadequate authority of the OCIO over Federal systems at Headquarters, and ineffective communication and cooperation among programs contributed to the MIS/DOEInfo security breach.

Competing Priorities

Competing priorities within and between the Department's programs frequently resulted in decisions being made that increased the risk of intrusion to the Department's systems. For example, although the OCIO had requested permission from the OCFO to perform authenticated scans of DOEInfo, officials from the OCFO's Office of Corporate Information Systems commented that they had concerns related to degraded performance and what they believed to be unnecessary system access. This precluded testing from occurring in a timely manner and outweighed the necessity to review the system to ensure that sensitive data, including PII, was properly secure. In preliminary comments on our report, OCFO officials informed us that an alternative testing process had been suggested. However, this testing still had not been completed by the OCIO at the conclusion of our fieldwork, nearly 3 months after MIS was placed back into operation following the breach. In addition, we noted that competing priorities may have impacted the Department's ability to complete the MIS upgrade in a timely manner. For example, the upgrade was significantly delayed by functionality issues between MIS and an underlying application. Because of this, MIS was allowed to operate in a vulnerable state until it was ultimately removed from the network following the breach.

We also determined that the Department did not act with sufficient urgency when determining how many individuals were impacted by the breach and notifying them accordingly. Specifically, the Department's Chief Information Officer was also the Senior Agency Official for Privacy, which may have hindered the response to the security breach. For example, employees within the OCIO were forced to balance the need to respond to and recover from the incident with the need to analyze forensic data so affected individuals could be identified and notified in a timely manner. We were told by OCIO officials that the organization responsible for incident response and recovery had also provided initial forensic information to the OCFO for analysis and identification of affected individuals. However, at some point, the decision was made by a senior OCIO official to focus solely on incident recovery and perform no additional work on providing information to the OCFO for analysis. As a result, conflicting priorities may have resulted in a less than fully effective and timely response in notifying individuals impacted by the breach. In response to our ongoing criminal investigation, the Department initiated additional efforts at our request to ensure that all affected individuals were identified. As a result of the Office of Inspector General's efforts, the Department identified more than 50,000 additional individuals impacted by the security breach but had not completed notifications to the affected individuals at the time of our review.

Lines of Responsibility

Issues related to vulnerability management and security testing were exacerbated by blurred lines of responsibility for application patching and maintenance of MIS. In particular, even though the system had been in operation for many years, there was apparent confusion as to which organization was responsible for ensuring that proper security was maintained. Although the OCIO had recently acknowledged ownership of MIS and began the security authorization process, it had not fully accepted all of its responsibilities for the system, such as patch management. To that end, we noted that the specific organizational responsibilities of shared support staff had not been documented – leading to the confusion we observed regarding work performed. We believe such actions created an atmosphere in which both the OCIO and OCFO

perceived the other was responsible for addressing system vulnerabilities, with no action being taken by either organization. To its credit, prior to the issuance of our report, the OCIO took action to identify and document the system-level responsibilities of support staff shared with the OCFO.

We also found that the Memorandum of Understanding used for systems hosted by the OCIO was in a standard format and was not tailored to each system for which it was executed. OCIO officials told us that they provided server maintenance and operating system patching, while system owners, such as the OCFO, were responsible for patching any applications that were installed on the servers. However, many program officials told us that they were unsure where their responsibilities began for systems hosted by the OCIO. We also noted that the Memorandum of Understanding did not include any corrective measures that could be taken by either party for noncompliance with the requirements of the document. Such alternatives could have allowed the OCIO to block or remove unpatched or otherwise insecure systems, such as MIS, from the network until they were properly secured. In preliminary comments to our report, OCFO officials noted that such actions did not apply to MIS because it was an OCIO system. However, we noted that following the breach the OCFO rebuilt the system and approached the OCIO to obtain agreement to return it to the operating environment. The OCIO concurred with the understanding that the system be placed on the Department's internal network. We believe that such actions contributed to the confusion we observed surrounding the responsibilities for MIS.

Urgency and Awareness

We determined that a lack of urgency regarding cyber security may have contributed to the MIS/DOEInfo security breach. For example, in December 2012, the MIS system was identified by the OCFO's Office of Corporate Information Systems as having numerous vulnerabilities and was in need of an upgrade to a newer more secure version. However, the OCFO and OCIO did not ensure the existing application upon which MIS was built was adequately secured while the upgrade was in the process of being implemented, leaving the system with numerous vulnerabilities, one of which was exploited during the breach. There was also confusion between the OCIO and OCFO regarding management of MIS; yet, there was no urgency to solidify system responsibilities and develop a path forward until January 2013, when the OCIO acknowledged its duties as system owner. Instead, both groups assumed it was the other's responsibility, leaving the system vulnerable and inappropriately managed.

Furthermore, the DOEInfo database had become increasingly complex – adding more than 30 interconnections with other applications since it was developed in 1994. Department officials, however, had not maintained an awareness of the operating environment. After the recent breach, the OCIO and OCFO were working together to identify and map out the full scope of the system, including connectivity to other systems. In comments on our preliminary report, OCFO officials stated that they were aware of and had properly managed all system interconnections to DOEInfo. However, our review identified at least two interconnected systems that were no longer being used, one of which had non-sensitive data taken from it during the breach. One senior OCIO official even commented that he was unaware the system existed, let alone that it

was the central repository for the Department's PII. Had the Department maintained a clear understanding of its operating environment, the need for enhanced security controls could have been identified and implemented, as appropriate.

Authority over System Operations

The *Federal Information Security Management Act of 2002* requires that the Chief Information Officer have direct authority and responsibility to ensure that the Department's information security policies, procedures and practices are adequate. However, because of certain delegations of authority, the Chief Information Officer was required to coordinate those efforts with the Senior Secretarial Officers. As a result, the authority of the Chief Information Officer had become limited due to the emphasis placed on program and staff office requirements rather than ensuring the security of the Department's information systems. Specifically, we noted during our review that OCIO officials had not been fully empowered to take systems that posed significant risk to the Department off the Headquarters network. We confirmed that no such authority existed despite the increased complexity of the Department's Headquarters network and reliability on the internet to accomplish business needs. Further, several individuals informed us that past management practices had been to not disrupt the business and mission requirements of the programs and staff offices that had systems hosted by the OCIO.

We believe the lack of a centralized authority over Federal systems at Headquarters to act in case of an emergent need adversely impacts the Department's ability to effectively minimize the risk of unauthorized access to and disclosure of sensitive information. We recognize the need to appropriately balance mission requirements against cyber security measures and to ensure operability for authorized access. However, we believe that an appropriate risk-based approach must consider the benefits provided to a select few against the risks to all of such a significant loss of sensitive information. Rather, outdated and unsecured systems like MIS were allowed to remain on the network even though the OCIO knew that continued operation significantly increased the risk that the Department's systems and information could be compromised. Without a defined, centralized authority to act in an emergent situation and resolve disputes, the Department may not be able to minimize the effect of future cyber security breaches.

Communication and Coordination

The Chief Information Officer and Senior Program officials are responsible for coordinating responsibilities to provide information security for systems and data that support the assets under their control. However, a lack of communication and cooperation within and between programs contributed to a culture wherein cyber security became secondary to ease of system access and completion of mission work. Several OCIO officials we met with during our review commented that they were frequently directed by programs to not implement tools or controls on systems because it would affect performance or make it harder for employees to do their work. We were also told that several of the Department's programs would not provide information to the Chief Information Officer about systems and risks even though that individual is ultimately responsible for risk acceptance authority over Federal systems at Headquarters. As such, the Department could not attest to the level of risk its systems face on a daily basis. Notably, following the July 2013 breach, the OCFO was one of only two programs/offices to provide the OCIO with requested information pertaining to systems containing PII.

Conversely, program officials stated that they frequently communicated information to the OCIO, as in the case of DOEInfo log anomalies and a drive space issue on the MIS server (Appendix 1), but would not receive a response as to whether there was a need for concern. Specifically, we noted that the OCIO had alleviated the space issue by deleting what it determined to be a data dump file created by the Department's forensic tool. However, the OCIO did not investigate whether that file was the reason for the loss of space prior to deleting it. Rather, it identified the file as the largest on the server and the quickest way to remediate the immediate issue and allow normal operations to resume. OCFO officials noted that the MIS server generally had more than sufficient disk space. As such, we questioned why the loss of space on a server that had never experienced a similar issue was not of higher concern. In short, we have reason to believe that the loss of space may have been the result of the attacker attempting to exfiltrate information and, with the proper analysis, communications and coordination, this could have been confirmed as suspicious activity, and the eventual loss of data may have been prevented.

Furthermore, a privacy official within the OCIO noted the privacy response for an unrelated cyber incident in January 2013, was confusing, frustrating and disorganized. Although a senior OCIO official stated at the time that a turnkey response plan would be established for future incidents, it was not developed and resulted in a similar confusing, frustrating and disorganized response to the recent breach. We believe strong leadership, a concerted effort, and willingness to move past the event to revamp the cyber security program and control environment could begin to rebuild trust throughout the Department. Certainly, the culture within the Department that minimized communication and coordination was not developed over a short period of time and, as such, will not be fixed overnight. However, the stovepipe approach to managing information systems and data has proven, as with the MIS breach, that continued failure to communicate and coordinate efforts could lead to significant negative mission impact and unauthorized loss of sensitive information.

Impact and Path Forward

Without improvements to the Department's information technology and management control environment in areas such as the use of Social Security numbers, internet accessibility, vulnerability management and continuous monitoring, the Department will continue to place systems containing sensitive information, including PII, at a higher than necessary risk of unauthorized disclosure. For example, we noted that the Department had identified additional high-risk systems containing PII that could be at risk of future compromise. These applications contained PII and protected health information, the loss of which could affect public safety and health especially to the Department's workforce. Although precautions to secure the compromised system had been taken subsequent to the breach, we believe immediate additional efforts are needed to strengthen the Department's cyber security posture, including reviewing the additional high-risk systems and taking necessary action to minimize the likelihood of future events.

Absent better protections, the Department could also continue to absorb the financial consequences that are related to recovering from breaches of data security. Alarming, we noted as many as 150,000 unique 9-digit records in the forensic data gathered after the event. Therefore, we believed the number of affected individuals significantly exceeded the 53,000

reported by the Department prior to our review. Having determined the potential for nearly three times the number of affected individuals during our review, we communicated our concern that the Department had not performed its due diligence in identifying all affected individuals and ensuring they were notified in a timely manner. In response to our analysis and briefing to the Deputy Secretary in September 2013, the Department's Chief Information Officer and Acting Chief Financial Officer stated that they believed many of the records included in the forensic data represented false positives, but estimated the number of individuals impacted to be over 104,000. In October 2013, the Department communicated the revised number of 104,179 affected individuals to its employees. The OCIO noted that, as of October 2013, the Department estimated it would spend approximately \$1.6 million for credit monitoring and labor costs associated with establishing a call center through which affected individuals could obtain additional information on the breach. We noted that additional costs may be necessary to support continued call center operations. In addition, the Department had incurred significant costs associated with the recovery and lost productivity – funds that could have been better spent supporting the Department's core missions. For instance, in October 2013, the Secretary authorized the use of up to 4 hours of administrative leave to all affected Federal employees to take action to correct issues associated with the event, an action we estimated could cost the Department an additional \$2.1 million in lost productivity.

We also found that breached information exceeded just names, dates of birth and Social Security numbers as initially reported by the Department. In particular, we noted through investigation or discussions with officials that select bank account numbers, places of birth, education, security questions and answers, and disabilities were also included in the loss of information. According to officials we spoke with, several employees had received notification that their PII had been compromised in both this and an earlier unrelated breach and noted that employee complaints demonstrated a loss of confidence in the Department's management. As the Department works to improve its relationships with the affected individuals, it must make an earnest attempt to ensure that notifications are made as quickly as possible.

RECOMMENDATIONS

Given the unprecedented extent of this security event and loss of PII, prompt and effective corrective actions are essential. In that respect, in addition to the actions recently initiated, we recommend that the Department's Chief Information Officer and Acting Chief Financial Officer, in coordination with the Acting Under Secretary for Nuclear Security, Acting Under Secretary for Science and Energy and Acting Under Secretary for Management and Performance:

1. Complete additional forensics reviews, as appropriate, to identify all types of data compromised and notify affected employees, dependents and contractors of compromised data in a timely manner in accordance with appropriate laws and regulations;
2. Identify all externally facing systems, determine if the continued external access is necessary, and remove access if not deemed essential;
3. Implement an effective continuous monitoring program, to include the performance of periodic in-depth authenticated reviews of each system, especially those that are externally facing;

-
4. Reconfigure the DOEInfo database tables to remove unnecessary or outdated information, remove Social Security numbers where possible, and protect those remaining Social Security numbers through the use of encryption or other security protocols as appropriate and in conjunction with Federal requirements;
 5. Clarify the authorities and responsibilities of the OCFO and the OCIO as they pertain to the ownership and management of the impacted systems;
 6. Develop an effective risk management approach that properly identifies weaknesses and costs of mitigation to allow senior management officials to effectively apply limited resources to minimize future events;
 7. Develop a process and central authority responsible for shutting down compromised or significantly vulnerable systems, at least on a temporary basis, to ensure minimal disclosure of national security, personally identifiable and other sensitive information; and
 8. Prepare a lessons learned report that can be shared across the complex.

MANAGEMENT REACTION

Management concurred with each of the report's recommendations and indicated that corrective actions had been taken or were planned to address the issues identified during our review. For instance, management commented that it had completed forensic reviews related to the breach and had notified nearly all of the individuals whose information had been compromised. In addition, management stated that it will remove Social Security numbers from DOEInfo, where possible, and protect the remaining numbers through the use of encryption or other security protocols. Management also committed to enhancing its continuous monitoring process, including conducting vulnerability assessments of DOEInfo and its connected services and applications.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 4.

TIMELINE OF EVENTS SURROUNDING THE MANAGEMENT INFORMATION SYSTEM SECURITY BREACH

Based on interviews with Department of Energy (Department) and contractor officials and reviews of supporting documentation, we established a timeline of events related to the recent breach of the Management Information System (MIS) and DOE Employee Data Repository (DOEInfo) database. In particular, we found:

- July 2, 2013: An application developer noticed an anomaly in the DOEInfo system logs while performing duties for the Office of the Chief Financial Officer (OCFO) related to investigating an unrelated programming error. The responsible group within the Office of the Chief Information Officer's (OCIO) Energy Information Technology Services (EITS) organization was notified so it could investigate further, because it has responsibility for the servers on which MIS and DOEInfo reside. The determination was made by an OCIO official that someone was repeatedly attempting to access the server running MIS. The developer told us that he did not receive any feedback on this issue from EITS.
- July 24, 2013: The MIS server was breached according to forensic analysis that was performed following the event.
- July 25, 2013: The OCFO application developer noticed that the MIS server had run out of drive space and was not responding to normal data requests. Officials from that office stated that this was an anomaly as the system generally had an ample amount of memory available. Again, EITS was notified. In this instance, no investigation was performed to determine the reason for the loss of space. Rather, the largest unnecessary data file on the server was deleted to allow the system to return to normal operation.
- July 26, 2013: Data was successfully exfiltrated from the DOEInfo database through MIS when hackers were able to elevate their privileges and run more than 600 queries against the system in a role that provided unlimited access to the database and other files on the MIS server.
- August 8, 2013: The data breach was identified, and MIS was taken offline.
- August 18, 2013: MIS was reintroduced to the Department's internal network after both the virtual machine and web application were rebuilt using a clean operating system and updated version of the application software.

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

To determine the circumstances that led to the July 2013 cyber security breach at the Department of Energy (Department) Headquarters.

SCOPE

The review was performed between September and December 2013, at the Department's Headquarters facilities in Washington, DC, and Germantown, Maryland.

METHODOLOGY

To accomplish our objective, we:

- Conducted over 35 interviews with Federal and contractor officials from the Offices of the Chief Information Officer and the Chief Financial Officer as well as other program and staff offices;
- Reviewed Federal laws and regulations related to controls over information technology security and privacy such as the *Federal Information Security Management Act of 2002*, Office of Management and Budget Memoranda and National Institute of Standards and Technology standards and guidance;
- Evaluated supporting documentation related to cyber security planning, development and management of the Department's Management Information System and the DOE Employee Data Repository database;
- Analyzed forensic data from the security breach to include data and database tables exfiltrated;
- Reviewed the relationships among the Office of the Chief Information Officer and Headquarters programs and staff offices; and
- Reviewed prior reports issued by the Office of Inspector General and the U.S. Government Accountability Office.

We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our objective. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our review. We did not rely on computer-processed data to satisfy our objective. We held an exit conference with the Chief Information Officer on December 6, 2013.

PRIOR REPORTS

- Evaluation Report on [*The Department's Unclassified Cyber Security Program – 2012*](#) (DOE/IG-0877, November 2012). The review identified weaknesses with access controls, vulnerability management, integrity of web applications, planning for continuity of operations and change control management. The weaknesses identified occurred, in part, because Department of Energy (Department) elements had not ensured that cyber security requirements were fully developed and implemented. In addition, programs and sites had not always effectively monitored performance to ensure that appropriate controls were in place. Without improvements to its unclassified cyber security program, including implementation of effective continuous monitoring practices and adopting processes to ensure security controls are in place and operating as intended, there is an increased risk of compromise and/or loss, modification and non-availability of the Department's systems and the information.
- Evaluation Report on [*The Department's Unclassified Cyber Security Program – 2011*](#) (DOE/IG-0856, October 2011). The review noted that the number of weaknesses identified represented a 60 percent increase over the previous year, and although some action had been taken, there was still additional action needed to further strengthen the Department's cyber security program. Specifically, the review revealed weaknesses in the areas of access controls, vulnerability management, web application integrity, contingency planning, change control management and cyber security training. The weaknesses identified occurred, at least in part, because Department elements had not ensured that cyber security requirements included all necessary elements and were properly implemented. Program elements also did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place. Without improvements to its unclassified cyber security program, such as consistent risk management practices and adopting processes to ensure security controls are appropriately developed, implemented and monitored, there is an increased risk of compromise and/or loss, modification, and non-availability of the Department's systems and information.
- Evaluation Report on [*The Department's Unclassified Cyber Security Program – 2010*](#) (DOE/IG-0843, October 2010). The review noted that although some action had been taken, there was still additional action needed to further strengthen the Department's cyber security program. Specifically, the review revealed weaknesses in the areas of access controls, configuration and vulnerability management, web application integrity, and security planning and testing. The weaknesses identified occurred, at least in part, because Department elements had not always ensured that cyber security requirements were effectively implemented, not had they adequately monitored cyber security performance. Plans of action and milestones were also not always used effectively to ensure that known security vulnerabilities were properly remediated. Without improvements to its cyber security program, Department systems and the information they contain are exposed to a higher than necessary level of risk.

- Audit Report on [*Protection of the Department of Energy's Unclassified Sensitive Electronic Information*](#) (DOE/IG-0818, August 2009). The review identified that some sensitive information at various sites was not encrypted, which included both stored and transmitted information, hardware was not properly secured, and programs and sites were still working to complete required Privacy Impact Assessments. These weaknesses were attributable in part due 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 to ensure that measures were in place to fully protect sensitive information. While some steps have been taken to address these identified weaknesses, additional effort is needed to help ensure that the privacy of individuals is adequately protected and that sensitive operational data is not compromised.

MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

December 4, 2013

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM:

ROBERT F. BRÉSE 
CHIEF INFORMATION OFFICER

ALISON L. DOONE 
DEPUTY CHIEF FINANCIAL OFFICER

SUBJECT: Inspector General's Draft Audit Report on "The Department of Energy's July 2013 Cyber Security Breach"

Thank you for the opportunity to comment on the Draft Audit Report, "The Department of Energy's July 2013 Cyber Security Breach". We have reviewed the report and concur with the management recommendations.

The recommendations outlined in the report will enable the Offices of the Chief Information Officer (OCIO) and Chief Financial Officer (OCFO), in coordination with our Program and Staff Offices, to take appropriate follow-up actions to improve DOE's cyber security posture.

Attachment A summarizes DOE management's response to the specific recommendations outlined in the report. Detailed technical comments from the OCIO and OCFO are contained in Attachment B.

If you have any questions or need additional information, please feel free to contact me at (202) 586-0166.



Printed with soy ink on recycled paper

Attachment A

MANAGEMENT RESPONSE

Inspector General's Draft Special Report on *The Department of Energy's July 2013 Cyber Security Breach*

Recommendation 1: Complete additional forensics reviews, as appropriate, to identify all types of data compromised and notify affected employees, dependents and contractors of compromised data in a timely manner in accordance with applicable laws and regulations.

Management Response: Concur

The Offices of the Chief Information Officer (OCIO) and the Chief Financial Officer (OCFO) have completed additional forensic reviews. In accordance with the Office of Management and Budget's (OMB) Memorandum M-07-16 and DOE Order 206.1 for source, content, method and target for notifying affected personnel, notifications have been completed for over 99% of the affected individuals. The OCIO has continued to exhaust all means of outreach to affected personnel, including but not limited to:

- Posting alerts and notices on internally and externally facing Energy web sites
- Generating log-in alerts
- Communicating directly with all internal and external organizations having affected personnel
- Providing a dedicated call center with a toll free number
- Leveraging commercial search services

The OCIO continues to work with other organizations, including government agencies and commercial search firms, to locate accurate contact information in order to notify the remaining less than 1% of the affected personnel.

Recommendation 2: Identify all externally facing systems, determine if the continued external access is necessary, and remove access if not deemed essential.

Management Response: Concur

The OCIO has been working with the Office of Health, Safety and Security (HSS) to complete a full assessment of all Internet facing systems on the DOE Trusted Internet Connection (TIC), with the goal of a near real-time understanding of vulnerabilities present on TIC systems.

The OCIO has engaged the Department of Homeland Security (DHS) to conduct scans of the entire DOE Internet Protocol (IP) space for vulnerabilities. DHS has a major program designed

Appendix 4 (continued)

to scan large network blocks for web application and other vulnerabilities. DHS has already scanned for specific vulnerabilities related to Content Management System vulnerabilities and provided reports on DOE's sites with vulnerable systems. The OCIO is following up with Program and Staff Offices (PSOs) regarding the results of DHS scans.

Recommendation 3: Implement an effective continuous monitoring program, to include the performance of periodic in-depth authenticated reviews of each system, especially those that are externally-facing.

Management Response: Concur

DOE is integrating continuous monitoring into its department-wide cybersecurity strategy. DOE is participating in DHS's Continuous Diagnostics and Mitigation (CDM) Program and is an "early engager" within the program, with plans to expand the program broadly across DOE in FY 2014. DOE elements report progress toward continuous monitoring goals through the Department's Business Quarterly Report (BQR) process. Additionally, the CIO is drafting implementation direction and guidance to achieve White House Cybersecurity Cross Agency Priority Goals. This direction and guidance will be reviewed by the Cyber Council and issued by the Deputy Secretary.

The OCIO and OCFO have also requested HSS to conduct initial and periodic authenticated scans of DOEInfo and its connected services and applications. Improvements to the real-time protection and continuous monitoring of DOEInfo and the underlying infrastructure are being implemented by the OCIO.

Recommendation 4: Reconfigure the DOEInfo database tables to remove unnecessary or outdated information, remove social security numbers (SSNs) where possible, and protect those remaining SSNs through the use of encryption or other security protocols as appropriate and in conjunction with Federal requirements.

Management Response: Concur

The OCIO and OCFO are partnering to conduct a detailed review of all services and applications with connections to DOEInfo. This review will include an evaluation and validation of the need for the collection and retention of employee data. The review will include an assessment of the security associated with the application or service connection to DOEInfo, as well as the security associated with the connected service and/or application itself. The review will also include an assessment of record retention requirements and the separation of historical records from active data.

Phase 1 will be completed by the end of January 2014 and involves the removal of all unnecessary or outdated information and removal of SSNs, where possible. Phase 2 will be completed by the end of May 2014 and will protect remaining SSNs through the use of

Appendix 4 (continued)

encryption or other security protocols as appropriate and in conjunction with Federal requirements. OCFO has already made several improvements to DOEInfo since the event:

- Changed all user and database connection passwords (August 20, 2013)
- Encrypted DOEInfo password table at rest (September 4, 2013)
- Forced DOEInfo password change on-line (September 4, 2013)
- Removed bad password strings from being stored. Storing only the date and time of the failure (September 17, 2013)
- Updated official leave forms to include digital signature capability and collect only the last four digits of the employee's SSN. The only affected page is the leave donation report used by DOE Payroll Office. Added a new ESS Admin role for leave donation so only the Payroll Office will see the ESS leave donation functions (September 19, 2013)
- Activated database auditing for all DOEInfo users coming in through the DOE Intranet and via tools such as Microsoft Access (October 1, 2013)
- Archived or deleted 152 tables that contained SSNs from the DOEInfo database (October 25, 2013)

Recommendation 5: Clarify the authorities and responsibilities of the OCFO and the OCIO as they pertain to the ownership and management of the impacted systems.

Management Response: Concur

Authorities and responsibilities of the OCFO and the OCIO as they pertain to the ownership and management of impacted systems will be formally documented by December 31, 2013.

Recommendation 6: Develop an effective risk management approach that properly identifies weaknesses and costs of mitigation, to allow senior management officials to effectively apply limited resources to minimize future events.

Management Response: Concur

Line managers are responsible for the effective risk management of systems under their authority and purview. Within the OCIO, the CIO has rescinded the delegation of system authorization and implemented weekly reviews of system risks under the line management authority of the CIO. These weekly reviews include discussion of inherited or transferred risks associated with hosting, housing and interconnect agreements. The OCIO will work with PSOs and HSS to coordinate insight and oversight of risk management. In addition, the DOE Cyber Council has tasked a working group within DOE to review management and technical best practices and to develop recommendations for propagating best practices across the DOE enterprise.

Recommendation 7: Develop a process and central authority responsible for shutting down compromised or significantly vulnerable systems, at least on a temporary basis, to ensure minimal disclosure of national security, personally identifiable and other sensitive information.

Appendix 4 (continued)

Management Response: Concur

System and application owner/operators are ultimately responsible for the security of their systems. The OCIO will review and update the Data Center and Systems Services Application Hosting Environment Memorandum of Agreements and Interconnection System Agreements to ensure roles and responsibilities are clearly documented by January 31, 2014. In addition, the authorities and process for identifying significantly vulnerable systems, communicating their vulnerabilities and status, shutting down or severing connections to these systems, and reactivating these systems after appropriate actions are taken to reduce or eliminate the risk will be formally documented by March 31, 2014.

Recommendation 8: Prepare a lessons learned report that can be shared across the complex.

Management Response: Concur

The OCIO and OCFO will prepare a lessons learned report by December 31, 2013.

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 applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or 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 that 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 our office at (202) 253-2162.

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://energy.gov/ig>

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