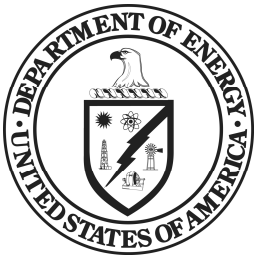

U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Audit Report

Department of Energy's Fiscal Year 2013 Consolidated Financial Statements

OAS-FS-14-03

December 2013

Department of Energy
Washington, DC 20585

December 12, 2013

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on the "Department of Energy's Fiscal Year 2013 Consolidated Financial Statements"

Pursuant to requirements established by the *Government Management Reform Act of 1994*, the Office of Inspector General engaged the independent public accounting firm of KPMG, LLP (KPMG) to perform the audit of the Department of Energy's Fiscal Year 2013 Consolidated Financial Statements.

KPMG audited the consolidated financial statements of the Department as of September 30, 2013 and 2012, and the related consolidated statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the years then ended. KPMG concluded that these consolidated financial statements are presented fairly, in all material respects, in conformity with United States generally accepted accounting principles and has issued an unmodified opinion based on its audits and the reports of other auditors for the years ended September 30, 2013 and 2012.

As part of this review, auditors also considered the Department's internal controls over financial reporting and tested for compliance with certain provisions of laws, regulations, contracts and grant agreements that could have a direct and material effect on the consolidated financial statements. The audit revealed certain deficiencies in internal control related to unclassified network and information systems security that were considered to be a significant deficiency. The following significant deficiency in the Department's system of internal controls is not considered a material weakness:

- Unclassified Network and Information Systems Security: Network vulnerabilities and weaknesses in access and other security controls in the Department's unclassified computer information systems continue to exist. The Department has taken steps to enhance its unclassified cyber security program, including increasing the high level visibility of cyber related issues, consolidating incident response services and capabilities, and working with programs and sites toward the effective implementation of a risk management approach.

The audit disclosed no instances of noncompliance or other matters that are required to be reported under applicable audit standards and requirements.

KPMG is responsible for the attached auditor's report and the opinions and conclusions expressed therein. The Office of Inspector General is responsible for technical and administrative oversight regarding KPMG's performance under the terms of the contract. Our review was not intended to enable us to express, and accordingly we do not express, an opinion on the Department's financial statements, management's assertions about the effectiveness of its internal control over financial reporting or the Department's compliance with laws and regulations. Our monitoring review disclosed no instances in which KPMG did not comply with applicable auditing standards.

We appreciated the cooperation of Department elements during the review.

Attachment

cc: Deputy Secretary of Energy
Acting Under Secretary for Nuclear Security
Deputy Under Secretary for Management and Performance
Deputy Under Secretary for Science and Energy
Chief of Staff
Deputy Chief Financial Officer

Audit Report: OAS-FS-14-03

http://www.energy.gov//cfo/reports/agency-financial-reports

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Independent Auditors' Report

The Inspector General, United States Department of Energy and
The Secretary, United States Department of Energy:

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the United States Department of Energy (Department), which comprise the consolidated balance sheets as of September 30, 2013 and 2012, and the related consolidated statements of net cost, changes in net position, and custodial activity, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 14-02 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the United States Department of Energy as of September 30, 2013 and 2012, and its net costs, changes in net position, budgetary resources, and custodial activity for the years then ended in accordance with U.S. generally accepted accounting principles.

Emphasis of Matters

As discussed in Note 7 to the consolidated financial statements, the Department has total direct loans and loan guarantees, net, of $15 billion and $13 billion as of September 30, 2013 and 2012, respectively, which are issued under the Federal *Credit Reform Act of 1990*. Subsidy costs of the direct loans and loan guarantees are intended to estimate the long-term cost to the U.S. Government of its loan program and include interest rate differentials, delinquencies, defaults, fees, and other cash flow items. A subsidy re-estimate is performed annually at September 30. Any adjustment resulting from the re-estimate is recognized as subsidy expense.

As discussed in Note 15 to the consolidated financial statements, the cost estimates supporting the Department's environmental cleanup and disposal liabilities of $280 billion and $268 billion as of September 30, 2013 and 2012, respectively, are based upon assumptions regarding funding and other future actions and decisions, many of which are beyond the Department's control.

As discussed in Note 18 to the consolidated financial statements, the Department is involved as a defendant in several matters of litigation relating to its inability to accept commercial spent nuclear fuel by January 31, 1998, the date specified in the *Nuclear Waste Policy Act of 1982*, as amended. The Department has recorded liabilities for likely damages of $21 billion and $20 billion as of September 30, 2013 and 2012, respectively.

Other Matters

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections be presented to supplement the basic consolidated financial statements. Such information, although not a part of the basic consolidated financial statements, is required by the Federal Accounting Standards Advisory Board who considers it to be an essential part of financial reporting for placing the basic consolidated financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic consolidated financial statements, and other knowledge we obtained during our audits of the basic consolidated financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Supplementary and Other Information

Our audits were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The consolidating information in the Consolidating Schedules section of the Department's 2013 *Agency Financial Report* is presented for purposes of additional analysis and is not a required part of the basic consolidated financial statements.

The consolidating information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic consolidated financial statements. Such information has been subjected to the auditing procedures applied in the audit of the basic consolidated financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic consolidated financial statements or to the basic consolidated financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the consolidating information is fairly stated in all material respects in relation to the basic consolidated financial statements as a whole.

The information in the Message from the Secretary, Message from the Chief Financial Officer, and Other Information section of the Department's 2013 *Agency Financial Report* has not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by *Government Auditing Standards*

Internal Control Over Financial Reporting

In planning and performing our audit of the consolidated financial statements, we considered the Department's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify certain deficiencies in internal control related to unclassified network and information systems security, described below and in more detail in Exhibit I that we consider to be a significant deficiency.

- *Unclassified network and information systems security* – We noted network vulnerabilities and weaknesses in access and other security controls in the Department's unclassified computer information systems. The identified weaknesses and vulnerabilities increase the risk that malicious destruction or alteration of data or unauthorized processing could occur. The Department should fully implement policies and procedures to improve its network and information systems security.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Department's consolidated financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a

direct and material effect on the determination of financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 14-02. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of compliance disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 14-02.

We also performed tests of its compliance with certain provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). Providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of FFMIA disclosed no instances in which the Department's financial management systems did not substantially comply with the (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

Department's Response to Findings

The Department's response to the finding identified in our audit is presented in Exhibit I. The Department's response was not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the response.

***Purpose of the Other Reporting Required by* Government Auditing Standards**

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the Department's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

December 10, 2013

Independent Auditors' Report
Exhibit I – Significant Deficiency

Unclassified Network and Information Systems Security
(Finding numbers reported in separate management letter)

The United States Department of Energy (the Department or DOE) uses a series of interconnected unclassified networks and information systems. Federal and Departmental directives require the establishment and maintenance of security over unclassified information systems, including financial management systems. Past audits identified significant weaknesses in selected systems and devices attached to the computer networks at some Department sites. The Department has implemented corrective actions to address many of the identified weaknesses at the sites whose security controls we, and the Department's Office of Health, Safety and Security, reviewed in prior years. However, at the time of our testing, corrective actions had not been fully completed. The frequency of network security weaknesses reported by KPMG has decreased when compared to the prior year weaknesses, but the number of weaknesses related to access control deficiencies in general information technology controls has increased since fiscal year (FY) 2012. The severity of these weaknesses remains consistent with prior year weaknesses. The Department recognizes the need to enhance its unclassified cybersecurity program and elevated unclassified cybersecurity to a material weakness in its *Federal Managers' Financial Integrity Act* assurance statement for FY 2013. Although the material weakness is not specific to financial systems, improvements are still needed in the areas of system and application access and related access privileges, password management, restriction of network services, configuration and vulnerability management, and system integrity.

Our FY 2013 audit disclosed information system security deficiencies similar in type and risk level to our findings in prior years. We identified similar weaknesses at sites where we had not reviewed security controls in the prior year. Specifically, we noted significant weaknesses and associated vulnerabilities for network servers and devices, desktop systems and business applications. We identified multiple instances of easily guessed login credentials or unrestricted access controls on network systems that could permit unauthorized access to those systems and their data. We also identified weak remote access controls in which multi-factor authentication had not been implemented for privileged users and access to sensitive information, such as personally identifiable information. In the area of account management and monitoring controls, when compared to weaknesses identified in our prior year's audit, we noted an increase in the frequency of weaknesses related to review, approval, provisioning and termination of administrative and user accounts that may increase the risk of malicious or unauthorized access to systems and data.

We identified deficiencies in configuration and vulnerability management on network server and desktop systems. Specifically, configuration and vulnerability management processes, including automated security update and patch management applications and other technical controls, were not fully implemented to identify, monitor and remediate system vulnerabilities. We found numerous instances in which critical security patches had not been applied in a timely manner to correct known vulnerabilities more than 30 days after the patches became available. We identified multiple server systems running operating system versions that were no longer supported by the vendor. We also noted that one site had not developed minimum security configuration policies and requirements for all systems. The affected systems included servers providing core network services and workstations used by financial application users and system administrators with privileged levels of access to financial applications and other network systems.

We also identified numerous weaknesses related to web application integrity as a result of design flaws in those applications. We identified web applications supporting financial processes that accepted insecure user authentication information or did not properly validate the form or content of input data against an application's database, which could result in unauthorized access to application functionality, sensitive data stored in the applications, and other network systems and applications.

While many of these weaknesses were corrected immediately after we identified and reported them to site management, deficiencies in cybersecurity processes and procedures have continued from prior years. We noted that multiple sites were continuing to develop and implement site-level Implementation Plans in accordance with the Department's Risk Management Approach to address cybersecurity weaknesses. However, these risk management enhancements were incomplete at the time of our testing. We also found that risk-based decisions, including evaluation and acceptance of risk, were not adequately documented at several sites to address residual risk, business justification, and mitigations.

The Department's Office of Inspector General (OIG) reported on these deficiencies in its evaluation report on *The Department's Unclassified Cyber Security Program - 2013*, dated October 2013. The OIG noted that the identified weaknesses occurred, in part, because Departmental entities had not ensured that policies and procedures were fully developed and implemented to meet all necessary cybersecurity requirements. The OIG reported that the Department continued to operate a less than fully effective performance monitoring and risk management program. The OIG noted that, contrary to Federal requirements, the Department's Plans of Action and Milestones were not always effectively used as a monitoring tool to report, prioritize and track cybersecurity weaknesses. The OIG also reported deficiencies in vulnerability and patch management at numerous sites in which vulnerable operating systems and applications were missing security updates and /or patches. The OIG further reported that weaknesses of this type directly contributed to the recent security breach of a Headquarters system containing significant amounts of personally identifiable information.

The identified vulnerabilities and control weaknesses in unclassified network and information systems increase the possibility that malicious destruction or alteration of data or unauthorized processing could occur. Because of our concerns, we performed supplemental procedures and identified compensating controls that mitigate the potential effect of these security weaknesses on the integrity, confidentiality and availability of data in the Department's financial applications.

During FY 2013, the Department had taken steps to enhance its unclassified cybersecurity program. To increase high-level visibility of cyber-related issues, a senior leadership council chaired by the Secretary of Energy was recently established. Additionally, the Department continues to consolidate incident response services and capabilities under the Joint Cybersecurity Coordination Center (JC3) and work with programs and sites towards effective implementation of a risk management approach.

Recommendation:

While progress has been made, continued efforts are needed to effectively manage the evolving nature of cybersecurity threats, including strengthening the management review process and monitoring of field sites to improve cybersecurity program performance; fully implementing revised and ongoing risk management processes; and expanding the use of automated tools in the resolution of the vulnerabilities and control weaknesses described above to properly configure, implement and update systems throughout the lifetime of those systems.

Therefore, we recommend that the Under Secretary for Nuclear Security, Under Secretary for Science and Energy, and Under Secretary for Management and Performance, in coordination with the Department and National Nuclear Security Administration Chief Information Officers, fully implement policies and

procedures to meet the Federal cybersecurity standards, that networks and information systems are adequately protected against unauthorized access, and that an adequate performance monitoring program is implemented, such as the use of periodic evaluations by Headquarters management, to improve the effectiveness of sites' cybersecurity program implementation. Detailed recommendations to address the issues discussed above have been separately reported to the cognizant management officials.

Management's Response:

The Department of Energy's Chief Information Officer (CIO) appreciates the opportunity to comment and the OIG's recognition of the Department's continued progress in addressing weaknesses and enhancing its unclassified cybersecurity program.

The Department continues its commitment to the protection of its information and information systems through a strong comprehensive Cybersecurity Program. Under the newly established Cyber Council chaired by Secretary Moniz and Deputy Secretary Poneman, activities are continuing to progress in effective risk-managed cybersecurity through maturing the Departmental Risk Management Framework (RMF). The information in this report will be brought forward to the Cyber Council for action and determination for path forward. In addition, the Under Secretaries, the Department CIO, NNSA CIO, and Program Support Offices will take appropriate follow-up action on specific findings, as well as to continue to work in the most effective way to improve the Department's cybersecurity posture.

The following efforts continue momentum in support of improving the Department's risk-managed cybersecurity posture through Federal mandated requirements.

- **Cybersecurity Cross-Agency Priority (CAP) Goals.** The Department is focusing on improving the cybersecurity posture through the use of three Cross Agency Priorities (CAP) goal programs: Trusted Internet Connection (TIC), Personal Identification Verification (PIV) Card Usage and Continuous Monitoring (CM). Scorecards are kept for each departmental element as well as the Department as a whole. The Department is actively participating in the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program and plans to expand the program during FY 2014 within DOE.

- **Information Sharing and Safeguarding (IS&S).** In a memorandum dated August 23, 2013, Secretary Moniz designated the Chief Information Officer (CIO) as the Department of Energy (DOE) Senior Agency Official (SAO) for Information Sharing and Safeguarding, thereby implementing Executive Order (E.O.) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." The Department has established an Information Sharing and Safeguarding Governance Board, chaired by the SAO, as well as a Secretary-designated Senior Insider Threat Officer who will lead efforts in new policy and programs.

- **Joint Cybersecurity Coordination Center (JC3).** Deputy Secretary Poneman signed the Memorandum for Heads of Departmental Elements on July 31, 2013, Subject: Cybersecurity Incident Management Improvements and the Joint Cybersecurity Coordination Center (JC3). This memorandum directs the consolidation of enterprise cybersecurity monitoring, information sharing, reporting, and federal enterprise incident response activities to the JC3 under the Office of the CIO. This will enhance the Department's ability to better manage future cyber security events, in a much more comprehensive manner.

In FY2014 the JC3 will expand enterprise incident response and management through the addition of personnel, tools, and the formalization of processes and metrics. Additionally, the program will increase enterprise monitoring, information collection, and advanced analytics as well as offering additional cybersecurity tools and services to customers Department wide. Based on recommendations from the Office of the CIO, the DOE Cyber Council is considering expansion of JC3 services like: the Cyber Federated Model (CFM) to increase cybersecurity information sharing; the Cooperative Protection Program (CPP) to increase situational awareness; and the DOE Enhanced Cybersecurity Services (DEX) to protect more sites with Intelligence Community informed filters and signatures.

IG Report No. OAS-FS-14-03

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 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.